GLI GLOBAL LEGAL INSIGHTS

Blockchain & Cryptocurrency Regulation

2023

Fifth Edition

Contributing Editor: **Josias N. Dewey**

glg global legal group

ENTERPRISE ETHEREUM ALLIANCE

Value Technology Foundation

WSBA WALL STREET BLOCKCHAIN ALLIANCE

CONTENTS

The law of the metaverse

Violetta Kokolus, Joshua Jackson & Jonathan Iwry
Ropes & Gray LLP

Introduction

The metaverse continues its rapid expansion while its participants and stakeholders attempt to keep pace in their efforts to grapple with and understand the legal framework that applies to it. There are several ways of interpreting the concept of the metaverse, but the term generally refers to a comprehensive online virtual network – one that uses virtual and augmented reality technology, as well as blockchain and digital assets, to create a persistent, immersive digital world where users can interact without being physically present. In theory, users of the metaverse will be able to shop for clothing and other goods, buy property, hold meetings, visit friends, attend concerts, and do anything else on a virtual basis that people might consider to be part of normal, day-to-day life. Leading tech companies have already begun preparing themselves for business opportunities in this new digital frontier. While it is unclear how influential the metaverse will prove to be, or what shape it will ultimately take, McKinsey & Co. estimates that the metaverse could generate up to $5 trillion in value by 2030.[1] In 2021, investment in the metaverse by private equity and venture capital hit $13 billion, more than doubling what it was in 2020.[2] One key characteristic of the metaverse that makes it promising is the prospect of integrating multiple emerging technologies – blockchain, cryptocurrencies, non-fungible tokens (NFTs), and the general concept of Web3 (a vision of a decentralised system for tomorrow's internet) – as the technological basis for metaverse activity.

Investors seem to view the metaverse as having almost limitless creative potential. But with that potential comes great uncertainty, as well as a whole host of legal questions that have yet to be resolved in their application to the metaverse. In fact, we are just encountering many of these legal questions for the first time, given that the forms that these issues take will depend in no small measure on how the metaverse evolves. While existing legal frameworks may apply in certain situations, in others, legal practitioners and courts are left to grapple with the application of existing laws that do not adequately contemplate the new technologies at issue or may not otherwise clearly apply. In still other situations, existing laws and legal frameworks may prove insufficient to address problematic conduct within the metaverse, thereby prompting passage of new laws and regulation.

In this chapter, we will explore the concept of the metaverse and the commercial opportunities it provides, and provide an overview of some of the key legal issues likely to arise as the metaverse continues to develop. We will also discuss the implications of these legal issues for parties considering whether to become stakeholders or participants in the metaverse.

Jurisdiction

The questions of whose law applies in the metaverse, and how to handle conflict of law disputes, will pose fundamental issues as legal authorities around the world seek to extend

their reach over the metaverse, and as private participants seek to resolve conflicts that arise within the metaverse. Furthermore, as private participants navigate the metaverse, they will require clear guidance as to which bodies of law apply to them and under what circumstances. This will be especially important for participants seeking to invest in the metaverse, who will have to contend with future assertions of jurisdiction by governmental entities and other private participants. Given how much uncertainty surrounds the state of the metaverse today, any ability to predict future lines of legal authority in the metaverse will have serious implications for parties interested in committing themselves to virtual platforms over the long term.

The application of jurisdiction within (or over) the metaverse raises many important questions, such as which countries' laws will apply in the metaverse, and how existing governmental entities will extend their governance online. Which courts' jurisdiction would a potential matter fall within? Will regulatory agencies in the real world govern the metaverse in similar ways to, and as extensions of, their real-world powers? Certainly, it is clear that the U.S. Securities and Exchange Commission (SEC) has authority over real work sales of securities involving parties in the United States. However, under what circumstances would sales of virtual interests in a virtual world be subject to SEC oversight? When an altercation in the metaverse between participants' avatars results in a harm to one avatar that would equate to breaking the law in the real world, would that altercation be handled by current tort law frameworks (which covers civil claims such as property damage, negligence or nuisance) or criminal law (involving illegal acts such as assault, murder, burglary, or rape)? Would it be possible for metaverse participants to waive or otherwise consent to (and thereby contract around) certain actions that cannot otherwise be waived or consented to under applicable law?

Similarly, how will conflicts of law be resolved in the metaverse? In theory, conflicts of law in the virtual world would be resolved according to the same rules that govern conflicts of law in any other context. But that depends on there being a well-defined framework for mapping participants, events, and territories in the metaverse onto existing bodies of law. Currently, "terms of use" in the form of end-user licence agreements between users and service providers are the dominant form of legal framework used to apply rules of governance in the metaverse, including to select preferred legal frameworks.

It is also possible that legal frameworks in the metaverse will be conceptualised in relation to existing geographic and legal territories. For example, the concept of territorial jurisdiction depends on the physical location of metaverse participants and would dictate that any legal issue that arose in the metaverse, but where the offenders are physically located in a particular country, would be subject to the courts of that country to decide the matter. Similarly, under the nationality principle, any legal issues that are committed in the metaverse by nationals of a given country, even if they are not physically situated in said country, would be subject to the laws of that country. Another possibility is that principles of extraterritorial jurisdiction will apply to the metaverse, such as those governing the law of the sea, Antarctica, or outer space, or that various regions of the metaverse will be treated as extensions of existing national territories and international bodies.

These questions will have serious implications for metaverse users seeking to avoid, mitigate, or resolve legal disputes. For example, if one party commits a tort by defrauding another, would straightforward principles of personal jurisdiction apply, giving authority to courts in the states where those parties reside? Would jurisdiction also be granted to the states from which those parties were accessing the metaverse? Likewise, how should

parties seeking to engage in a transaction involving virtual property take these issues into account in drafting their contractual choice of law provisions? The lack of guidance as to these issues could affect investor confidence and other market activity in the metaverse: parties who are concerned as to the current uncertainty involving virtual jurisdiction might be more risk-averse when considering whether and how to engage in business in or relating to the metaverse. As the use of the metaverse expands, it will likely take a series of court cases or comprehensive legislation to fully resolve the issues that will arise around legal jurisdiction in the metaverse.

Anti-money laundering

The metaverse provides a new frontier for financial transactions because of its inclusivity and lack of intermediaries. The internet as a whole is not subject to any one regulatory framework – and as things stand at present, neither is the metaverse. However, the existing lack of legislation and regulatory oversight poses a high risk of there being lack of recourse in the event of business fraud in the metaverse.

Some are hopeful that the application of blockchain technology to financial activity will help to make transactions in the metaverse more secure. Unlike traditional financial transactions, blockchain transactions are (at least in theory) immutable and traceable. Yet experience paints a different picture: in 2021, cryptocurrency-linked crime surged to a record high – illegal addresses received $14 billion in digital currencies, up 79% from the previous year.[3] Different countries have taken entirely different approaches to regulating cryptocurrencies as an asset class. Some, such as El Salvador, have chosen to accept Bitcoin as legal tender, while others, such as China, are banning entire sectors of crypto services.

The United States sits somewhere in the middle of the spectrum, with President Joe Biden's recent Executive Order instituting a broad call to action on digital asset development rather than seeking to prescribe a detailed framework.[4] In particular, President Biden's Executive Order highlights the weaknesses presented by jurisdictions that have not set sufficient standards: "Illicit actors, including the perpetrators of ransomware incidents and other cybercrime, often launder and cash out of their illicit proceeds using digital asset service providers in jurisdictions that have not yet effectively implemented the international standards set by the inter-governmental Financial Action Task Force (FATF)."

Additionally, the Anti-Money Laundering Act of 2020 (AMLA) expanded the definitions of "money transmitting business" and "financial institution" under the Bank Secrecy Act to include business involved in the exchange or transmission of "value that substitutes for currency".[5] In October 2021, the FATF – an intergovernmental organisation that develops standards to combat money laundering and terrorism financing – updated its guidance on virtual assets and virtual asset service providers, which could have implications for regulation of the metaverse.[6] The updated guidance outlines the need for countries, virtual service providers and other entities that leverage digital assets to understand the money laundering and terrorism financing risks associated with their activities and suggests appropriate mitigating measures to address them. If participants in the metaverse intend to introduce cryptocurrencies and other blockchain technologies into their dealings in the metaverse – and there is every reason to believe that they will – this raises important questions as to how existing regulation surrounding these technologies will apply and adapt to the metaverse.

Another important factor to consider is the prospect of artificial intelligence (AI)-assisted enforcement: advances in financial services technology may enable AI products to enhance the security of financial transactions (in the metaverse and elsewhere) by screening customers against global watchlists and categorising them by risk level,[7] perhaps supplementing or

eventually replacing Know Your Customer (KYC) requirements. This raises important questions as to how to balance the value of preventing fraud against the value of maintaining the inclusivity and access the metaverse brings to people traditionally left out of complex financial projects. And with advancements such as AI possibly supplementing or replacing AML/KYC disclosure laws, regulators will also have to consider how to ensure that AI is applied effectively, equitably, and with minimal cost to the law-abiding users whose transactions these advancements are intended to benefit.

Token issuances

The prospect of whether and how governments will regulate cryptocurrencies looms over the decisions that stakeholders face as to how to issue and use those products. Given the outsized role that cryptocurrencies and NFTs have played and will continue to play in the metaverse, platforms are likely to go to great lengths to ensure legal compliance in issuing crypto-backed tokens for use in transactions in the metaverse.

Token issuance is one of the most important aspects of blockchain-related technologies such as NFTs and cryptocurrencies, and will likely have a significant effect on the metaverse as well. Token issuances are introductions of new tokens into an existing system on a blockchain. This typically involves the creation of new tokens within a given cryptocurrency, though it can also involve the tokenisation of other, non-cryptocurrency assets. It will be important for platforms in the metaverse to regulate the supply of cryptocurrencies so as to ensure a secure and stable ecosystem in which to conduct business on the blockchain. This includes managing the introduction of new tokens into their existing supply – and even, in some cases, removing excess tokens to prevent inflation (also called "cryptocurrency burning").

A major question is whether crypto coins and NFTs will inspire new regulations, assimilated into existing securities regulations (for example, by being treated as investment contracts), or left largely unregulated with minimal guidance for stakeholders. What general rules and policies will regulatory agencies issue to address the issuance of NFTs and related technologies? Will new regulations come to treat tokens in the metaverse as constituting a distinct type of transaction with new legal standards, as a new subtype of existing transactional mechanisms, or as an open category best left to the parties involved to decide through private ordering?

Moreover, given that the computational activities required for certain cryptocurrency- and NFT-related technologies to function (also called "mining") are energy intensive and environmentally costly, it is possible that environmental regulatory agencies will push to limit, or at least regulate strictly, the amount of mining on the metaverse in general or by particular parties.

Increased attention is being given to the environmental impact of cryptocurrency activity. In June 2022, for example, the state Senate of New York passed a bill to counteract the growing use of fossil fuel by power plants for cryptocurrency mining, both by requiring research into the environmental impact of cryptocurrency mining within the state and by requiring an assessment, and by inducing a two-year moratorium on new and renewed air permits for plants engaging in cryptocurrency mining.[8] American political officials such as Elizabeth Warren have also suggested the possibility of regulating cryptocurrencies for environmental reasons, which the Chinese government cited as one of its reasons for banning domestic cryptocurrency mining.[9] It remains to be seen whether these concerns will affect the use of cryptocurrency in the metaverse, be it by influencing the general availability of cryptocurrency in the metaverse or by creating new rules or disincentives for the use of cryptocurrency by metaverse users.

Real estate

Virtual real estate in the metaverse has skyrocketed in popularity within the last year. It is common for metaverse platforms to allow users to buy, rent and invest in real estate that exists only within the virtual world. This development has to some extent mirrored the physical real estate industry, with companies offering mortgages to finance the purchase of virtual property and investors seeking the best virtual location in a metaverse. However, virtual real estate is distinct from physical real estate in two important aspects. First, though blockchain technology theoretically allows for "true" ownership of virtual property, metaverse platforms are typically governed by terms of use, which fall under the purview of contract law rather than property law.[10] However, in areas of the metaverse regulated by a decentralised autonomous organisation (DAO), virtual residents could have voting rights and potentially play a role in establishing and updating virtual property rules. Second, the metaverse comprises a multitude of private platforms, and there is no guarantee that any given platform used to invest in virtual real estate will be scalable and sustainable for the future, or able to successfully integrate with the rest of the metaverse. Citi has warned that a computational efficiency improvement of over 1,000 times today's levels would likely be needed to enable the seamless transfer of data on the scale that was originally envisioned for the metaverse.[11]

As things stand today, arguably, metaverse platforms and assets, including virtual real estate, fall under the purview of contract law (or the rules of a DAO) rather than property law. How will the multitude of corporations that constitute the metaverse create a universal system to protect metaverse property values and prevent digital property duplicates? The real-world equivalent is done through physical scarcity and the title record-keeping system; it remains to be seen whether a similar system will be created within the metaverse.

Intellectual property

The metaverse promises to create a new dimension of online economic activity, especially for the creator economy, and participants in the metaverse will therefore need to be mindful of how to monetise and protect their intellectual property (IP) rights. The decentralised nature of the metaverse poses a challenge to brands and IP owners looking to enforce their rights. In the physical world, companies and brands can level their concerns against a person, business, or website for their individual IP violations. By contrast, the decentralised nature of blockchain – and the lack of a singular source in which to compel "deleting" IP infringements – results in an entirely new terrain for IP enforcement with no single point of authority, such as a hosting provider, that can take down infringing content. Further complicating matters, once content is on the blockchain, it cannot be deleted; it is there for ever.

Other questions arise as to what types of creations and products will fall under IP laws in the metaverse, and, perhaps more importantly, what entities will enforce these laws. How will law enforcement authorities enforce IP laws given the decentralised nature of blockchain and lack of singular source for accountability? To what extent will regulators' efforts to prevent IP infringements be limited by the nature of the blockchain – and could the blockchain's strength in permanently recording any and all related transactions, legal or otherwise, pose a weakness in certain instances? Will the copyright doctrine of "fair use" apply in a similar manner? It is possible that a safe harbour and takedown process resembling that of the Digital Millennium Copyright Act (DMCA) will be crafted and implemented to apply in the metaverse.

In theory, traditional IP law applies to activities and entities that exist in the metaverse. But the unique terrain of the metaverse makes it difficult to predict how the principles of IP law will be implemented in practice. Consider a recent case involving the well-known Birkin

handbag. In December 2021, NFT creator Mason Rothschild sold a set of NFTs containing digital depictions of Birkin bags, called "MetaBirkins", for $42,000. Hèrmes sent Rothschild a cease-and-desist letter alleging trademark infringement. NFT exchange OpenSea responded by removing the MetaBirkins from its platform, but Rothschild has continued to sell them through his website. Hèrmes filed a claim against Rothschild in federal court in January 2022, with Rothschild defending the sale of his MetaBirkins as artistic works protected by the First Amendment.[12] NFTs have already been the subject of a number of IP-related disputes; given that NFTs are likely to play a significant part in business transactions in the metaverse, these issues in particular are sure to spill over into, and perhaps pose fundamental questions for, the possession, use, and transfer of IP on metaverse platforms.

Musicians have already begun hosting live performances in the metaverse, and VR-related artistic activity is only going to become more frequent. The unique features of the metaverse may create an entirely new context in which artists draw on familiar images, symbols, and other existing works in sharing in their own creations. As such, the metaverse may blur the line in trademark law between constitutionally protected artistic expression and display of commercial symbols – not to mention the line in copyright law between copyright infringement and valuable commentary – in new ways.

There is currently no easy way to monitor the metaverse for infringing content. IP searching and monitoring services generally do not have the capability to see or scrape content in Web3 platforms, and major search engines are unlikely to capture blockchain code in their common law web searches. However, in the future, specialised tools may be developed to monitor the metaverse for IP infringement. Further, like in traditional IP spaces, standard-setting organisations may agree on fair, reasonable, and non-discriminatory terms to create value through IP licences applicable to metaverse applications, and those licences are likely to be enshrined in smart contracts. Similarly, due to the ubiquity of open-source software in the metaverse, popular open-source protocols may arise based on the collective wants and needs of participants in the metaverse community.

Crowdfunding

One of the most interesting and widely heralded possible applications of the metaverse is the use of decentralised platforms to facilitate crowdfunding. While there are many rules that govern the offering of securities in the United States and elsewhere, it is worth noting that the current SEC rules under Regulation Crowdfunding require all transactions to take place online through an SEC-registered intermediary – either a broker-dealer or a funding portal.[13] These intermediary platforms are intended to act as gatekeepers by vetting fundraising efforts and identifying suspicious activity.[14]

A fundamental question is how these and other regulations will transfer to the metaverse, a powerful fundraising platform that utilises cryptocurrency and can bypass censorship to facilitate large-scale decentralised decision-making activity. By way of contrast, platforms such as GoFundMe and Kickstarter have nullified crowdfunded funds in the past due to terms of use violations or media scrutiny. Yet DAOs, smart contracts, and similar digital mechanisms at work in the metaverse may render these sorts of restrictions practically impossible. Accordingly, it will be important to consider how existing rules regarding the maximum crowdfunding amount allowed per business (currently $5 million/year), geographic restrictions (countries that are being sanctioned), and anonymity in crowdfunding will carry over to the metaverse.

If the use of intermediary platforms will no longer be necessary (or feasible), which entities will play the role of gatekeepers when dealing with large-scale collective activity in the metaverse? For example, how will regulatory bodies carry out their gatekeeping functions in light of autonomous smart contracts that can execute instantly without manual checkpoints/action? How will governments enforce current crowdfunding rules given the ease with which contributing parties can shield their identities?

Data and privacy

Extensive collection of personal and biometric data is likely to be pervasive in the metaverse. The sharing of data will be the cornerstone of an interoperable, virtual environment where participants and their digital personas and assets will be usable and tradeable across the different corners of the metaverse. The metaverse will open up new categories of our personal data for processing, including facial expressions, gestures and other types of avatar-generated reactions, and this data is likely to be very valuable to stakeholders operating in the metaverse. What laws will govern the collection, sharing and use of data across the metaverse? The laws of a particular state? Applicable federal privacy laws? The General Data Protection Regulation (GDPR) or other international regulations? Will there be a single overarching "privacy policy" governing the metaverse, or will there be varying policies depending on which realm of the metaverse someone is in? While current privacy and data security legal frameworks will certainly apply, the decentralised and largely permissionless nature of the metaverse could make it difficult to ascertain who owns or controls data. The clash between the online collection of personal data on the one hand, and the aspiration to protect privacy on the other, will have significant implications for the strength of privacy protections within the metaverse.

The need to balance collection of data and respect of privacy – and the inevitable overlap between distinct government entities – poses difficult questions. How will nations' biometric privacy laws apply in the metaverse, and which regulatory agencies will be responsible for compliance with those laws? How will national and international consumer privacy laws (e.g., California's Consumer Privacy Act, the EU GDPR) apply, and which regulatory agencies will be responsible for compliance? For avatars, do we look to the location based on the person operating the avatar, or do we look at the avatar itself, since it is the avatar's data that will be processed?

Consumer protection

The explosion of metaverse platforms and companies presents a variety of challenges to existing antitrust enforcement and consumer protection laws. Collaboration will be a cornerstone of the metaverse, as the metaverse is, by definition, a multi-tenant environment. Of course, collaboration amongst competitors may invoke antitrust concerns, and the larger technology companies may be perceived as leveraging their position to assert unfair control in the metaverse. With numerous companies seeking to establish dominance in the virtual realm, new regulations will likely need to address the balance between a competitive marketplace of metaverse platforms and the possible emergence of a singular "metaverse". This presents various questions as to whether existing consumer protection laws sufficiently address the likely manifestations of an anticompetitive marketplace, including data privacy violations, digital currency frauds, and IP infringements.

How will antitrust laws and regulations be enforced against companies and platforms for actions occurring in this new "reality"? What types of crimes and violations will regulatory

bodies level against metaverse companies? How will antitrust laws and agencies balance the duelling conceptions of a competitive marketplace of "metaverses" and a singular, dominant "metaverse?" And will the proprietary source code of metaverse platforms be classified as "corporate trade secrets" or receive other legal classifications that could halt the creation of a singular metaverse based on open-source code?

Artificial intelligence

As described earlier, AI is increasingly being considered a means of enhancing the security of digital financial transactions. This represents just one of many ways in which AI has the potential to influence activity in the metaverse, all raising numerous questions as to how to increase consumer protection, respect privacy, and navigate the many trade-offs of what is still a relatively new form of technology.

One way in which AI could affect the metaverse is through the introduction of what are called "soft laws", or lawlike guidelines that establish norms of conduct without being legally binding or having legal consequences. The use of soft law is already being explored in other contexts involving AI and other new technologies. In April 2020, for example, the Federal Communications Commission (FCC) made use of soft law by issuing an order to open the entire 6 GHz band to unlicensed use by Wi-Fi devices, citing their desire to harness the economic value created by Wi-Fi networks in the United States.[15]

Advocates believe that soft law can be used as a way of helping to encourage coordination across the private sector, without stifling innovation or tethering private participants to technologies that will quickly become outdated. A report from The Brookings Institution's Artificial Intelligence and Emerging Technology Initiative calls for the use of soft law in regulating AI-related spaces, arguing that it would be more sensible to set soft industry guidelines than to task "one or more government agencies with the rulemaking and oversight extensive enough to cover all of the many applications and industries where AI will be used".[16]

The use of soft law could influence the ways in which AI is used in online environments such as the metaverse, but it also serves as an example of how soft law could be used to guide the development of the metaverse more broadly. With government bodies looking to establish norms of good governance across the digital landscape without committing the private sector to overly rigid rules, it is quite possible that the coming years will see a rollout of soft law principles for online participants. This could benefit stakeholders in the metaverse by helping to establish stable guidelines; it could also run the risk of increasing uncertainty, or simply being ineffective, by virtue of those guidelines not being legally binding. Whether the use of soft law will extend to the metaverse, and which government bodies would be responsible for them, remain open questions.

Conclusion

Several key themes loom over the increasing movement of law into the metaverse. First, will government regulators adapt existing laws and regulatory frameworks to the metaverse, or will they create new ones entirely? For example, will the existing laws of real property be mapped on to the metaverse, such that regions within the metaverse will be conceptualised in terms of landownership, or will regions within the metaverse be treated as their own distinct type of entity? Second, which aspects of the metaverse's digital landscape, and which technological innovations at work in the metaverse, pose the biggest challenges to the existing regulatory regime? The third question, and perhaps the most fundamental: how will government regulators decide to balance the inherently private, decentralised, and clustered

nature of the metaverse with the goal of a unified and well-regulated digital domain? Accordingly, what steps can private participants in the metaverse take to ensure compliance and protect their interests as they navigate this new and largely uncharted digital terrain?

These themes are in some ways quite simple, but the details of their application will be exceedingly complex and have yet to be determined. How lawmakers choose to answer these questions will have fundamental effects on the new digital frontier as a whole and will be felt by parties across the metaverse. For entities seeking to participate in the metaverse, proactively considering the legal risks and finding means to mitigate them in the midst of a developing regulatory landscape will be critical to thriving in the metaverse.

* * *

Endnotes

1. McKinsey & Company, "Value Creation in the Metaverse" (2022), available at https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf.
2. *Id*.
3. Mengqi Sun and David Smagalla, "Cryptocurrency-Based Crime Hit a Record $14 Billion in 2021", *Wall Street Journal* (Jan. 6, 2022), available at https://www.wsj.com/articles/cryptocurrency-based-crime-hit-a-record-14-billion-in-2021-11641500073.
4. The White House, "Fact Sheet: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets" (Mar. 9, 2022), available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets.
5. Financial Crimes Enforcement Network, "The Anti-Money Laundering Act of 2020", available at https://www.fincen.gov/anti-money-laundering-act-2020.
6. FATF, "Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers" (June 2017), available at https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.
7. Deloitte and United Overseas Bank, "The Case for Artificial Intelligence in Combating Money Laundering and Terrorist Financing", available at https://www2.deloitte.com/mm/en/pages/financial-advisory/articles/the-case-for-artificial-intelligence-in-combating-money-laundering-and-terrorist-financing.html.
8. Michael Hill and Jennifer Peltz, "Landmark Bill to Limit Energy Intensive Cryptomining Passes New York Legislature", PBS (June 3, 2022), available at https://www.pbs.org/newshour/economy/landmark-bill-to-limit-energy-intensive-cryptomining-passes-new-york-legislature.
9. Jeffrey M. Kelly and Jeffrey E. Joseph, "Crossing the Wires of Energy and Cryptocurrency Policy: U.S. Congress Investigates the Environmental Impact of Crypto Mining", *National Law Review* (Feb. 4, 2022), available at https://www.natlawreview.com/article/crossing-wires-energy-and-cryptocurrency-policy-us-congress-investigates.
10. Joao Marinotti, "Can you Truly Own Anything in the Metaverse? A Law Professor Explains How Blockchains and NFTs Don't Protect Virtual Property", *The Conversation* (Apr. 21, 2022), https://theconversation.com/can-you-truly-own-anything-in-the-metaverse-a-law-professor-explains-how-blockchains-and-nfts-dont-protect-virtual-property-179067.

11. Citi GPS, "Metaverse and Money: Decrypting the Future" (Mar. 2022), available at https://ir.citi.com/gps/x5%2BFQJT3BoHXVu9MsqVRoMdiws3RhL4yhF6Fr8us8oHaOe1W9smOy1%2B8aaAgT3SPuQVtwC5B2%2Fc%3D.
12. *Hèrmes International, et al. v. Mason Rothschild*, No. 22-cv-384 (JSR) (S.D.N.Y. Jan. 14, 2022).
13. U.S. Securities and Exchange Commission, "Regulation Crowdfunding" (Aug. 24, 2022), available at https://www.sec.gov/education/smallbusiness/exemptofferings/regcrowdfunding.
14. U.S. Securities and Exchange Commission, "Press Release: SEC Charges Crowdfunding Portal, Issuer, and Related Individuals for Fraudulent Offerings" (Sep. 20, 2021), available at https://www.sec.gov/news/press-release/2021-182.
15. F.C.C., In the Matter of Unlicensed Use of the 6 GHz Band, Expanding Flexible Use in Mid-Band Spectrum Between 3.7 GHz and 24 GHz, ET Docket No. 18-295 and GN Docket No. 17-183, FCC 20-51 (Apr. 24, 2020).
16. John Villasenor, "Soft Law as a Complement to AI Regulation", The Brookings Institution (July 31, 2020), available at https://www.brookings.edu/research/soft-law-as-a-complement-to-ai-regulation.

* * *

Disclaimer

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or any of its or their respective affiliates. This chapter is for general information purposes and is not intended to be and should not be taken as legal advice.

* * *

Acknowledgment

The authors would like to thank Melissa Bender for her contribution to this chapter. Melissa is a partner in Ropes & Gray's asset management group and chair of the cryptocurrency and blockchain working group. She can be reached at melissa.bender@ropesgray.com.

Violetta Kokolus
Tel: +1 212 596 9085 / Email: violetta.kokolus@ropesgray.com
Violetta Kokolus is a partner in Ropes & Gray's intellectual property transactions group in New York. She advises on complex technology, intellectual property transactions, as well as critical IP and privacy and cybersecurity aspects of mergers & acquisitions transactions across various industries.

Joshua Jackson
Tel: +1 617 951 7860 / Email: joshua.jackson@ropesgray.com
Joshua Jackson is a senior associate in Ropes & Gray's technology transactions group. He advises public and private companies, investors and universities in a variety of transactions where technology and intellectual property are the fundamental drivers.

Jonathan Iwry
Tel: +1 617 951 7456 / Email: jonathan.iwry@ropesgray.com
Jonathan Iwry is an associate in Ropes & Gray's corporate practice in Boston. He advises on transactional matters for a variety of clients, with a focus on intellectual property and life sciences. He has published articles and written on various topics involving law, policy, and the ethics of emerging technologies.

Ropes & Gray LLP

Prudential Tower, 800 Boylston Street, Boston, MA 02199-3600, USA
Tel: +1 617 951 7000 / URL: www.ropesgray.com

www.globallegalinsights.com

Other titles in the **Global Legal Insights** series include:

AI, Machine Learning & Big Data
Banking Regulation
Bribery & Corruption
Cartels
Corporate Tax
Employment & Labour Law
Energy
Fintech
Fund Finance
Initial Public Offerings
International Arbitration
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Pricing & Reimbursement

GLI GLOBAL LEGAL INSIGHTS