



HOLD YOUR HORSES



BY
CAROL VAN CLEEF

CEO of Luminous Group, LLC.

THE FUTURE OF WEB3 DEPENDS ON CAREFUL REGULATORY APPROACHES

By Duane Pozza & Lauren Johnson



HOLD YOUR HORSES

By Carol Van Cleef



WEB3 IS COMING FAST, AND REGULATION NEEDS TO KEEP PACE

By Sean Stein Smith



WEB3 IN TRANSITION AND PARTICIPATORY REGULATION

By Fabio Bassan



INSURANCE'S ROLE IN THE REGULATION OF WEB3 THROUGH DE-RISKING

By Jessica Chapman



THE TOKENIZATION OF CONSUMER SURPLUS: NEW ANTITRUST TOOLS IN WEB3 MARKETS

By Kelly Fayne & Elise Nelson



INFUSE DIGITAL ASSETS TO JUMPSTART FINANCIAL LITERACY IN AMERICA'S EDUCATION SYSTEM

By Cleve Mesidor & Mali Smith



HOLD YOUR HORSES

By Carol Van Cleef

Web3 is not lawless territory. Regardless of how the term is defined or conceptualized, a number of existing laws and regulations already clearly apply – in some cases to the activities being conducted in Web3, in other cases to the underlying technologies supporting it and in yet other cases to those engaging with Web3. Overtime many other laws and regulations will be adapted, much like the process we have seen occur repeatedly when new technologies begin to gain traction. When the need for specific changes in law or regulation is identified the pace at which such actions ultimately will be taken – whether to add, revoke or amend – will occur more slowly than may be desired. In the meantime, success or failure in Web3 will depend on understanding what applies now and anticipating future changes.

Visit www.competitionpolicyinternational.com for access to these articles and more!

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.



Web3 is not lawless territory. Regardless of how the term is defined or conceptualized, a number of existing laws and regulations already clearly apply – in some cases to the activities being conducted in Web3, in other cases to the underlying technologies supporting it or in yet other cases to those engaging with Web3. Sometimes, it may not seem as clear what, if any, law, or regulation applies to a particular issue that arises in Web3. But, jumping to a quick conclusion that nothing applies may ultimately be costly and could have real consequences, including lawsuits, the collapse of the business, expensive fines, or even jail.

This dilemma is not new. Applications of new and evolving technologies not infrequently present challenges to existing legal and regulatory constructs. However, the unique characteristics commonly associated with Web3 – regardless of which working definition is used – require a measured approach when venturing into and staking out a claim in this rapidly expanding virtual territory.

Undoubtedly, overtime, some existing laws and regulations will need to be adapted, a practice we have seen occur repeatedly as new technology-driven business models gain traction. When the need for a specific change in law or regulation is identified the pace at which such change will be made – whether to add, revoke or amend – may be slower than desired. Rarely, at least in the U.S., will such changes be preemptive and almost never will they be made quickly.

Participating in the development of new or adaptation of existing laws, regulations or legal principles should be a priority when clear gaps are identified. The pace at which lawmakers and regulators focus on Web3 will be dictated in part by the rate of adoption however it is measured – number of users, number of applications, dollars spent, or some other metric. Typically, new laws are made in the wake of a crisis. In the end, policy makers are most likely to react after – not before – constituents get hurt physically or financially. But not every crisis results in new laws, and what happens next is often a function of not only how many constituents are harmed but also how vocal and influential the interested lobbies are. Importantly such lobbies may not be limited to industry or consumers but often include regulators. Education is also critical as many, for example members of the U.S. Congress, still face a steep

learning curve on the wide range of issues that ultimately comprise Web3.²

Regulators walk a finer line – sometimes. However, they tend to be much more proactive, seeking to protect their reputations in the face of growing storm clouds. This defensive posturing is a skill honed over many years from watching the accumulation of clouds portending past crises, hints of trouble for entities they supervise and/or a potential loss to Congressional constituents. For example, while the FTX collapse may not have been entirely foreseeable, federal banking regulators had been taking steps for months to erect a wall high enough to protect themselves and the banking industry for which they are responsible from a variety of potentially controversial issues surrounding cryptocurrencies.³ Although the regulators did not fully isolate themselves from congressional criticism, they created a substantial record of proactive steps that could serve as a shield to defend themselves if and when members of Congress in their watchdog roles start asking questions.⁴ We should expect a similarly cautious approach to be taken as banks enter Web3 and attempt to take advantage of the opportunity to develop more efficient and innovative products.⁵

“Undoubtedly, overtime, some existing laws and regulations will need to be adapted, a practice we have seen occur repeatedly as new technology-driven business models gain traction

In the meantime, individual successes or failures in Web3 will depend on understanding what applies now and appropriately anticipating future changes. Failure to comply with applicable laws can lead to civil or criminal prosecutions, especially when money or value is being exchanged. Addressing in early stages whether the tokens being used to facilitate activity in Web3 as a security or a non-securi-

2 See e.g. <https://www.coindesk.com/consensus-magazine/2023/01/23/rep-tom-emmer-crypto-and-web3-the-ownership-economy/?outputType=amp>.

3 See e.g. <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20230103a1.pdf>.

4 See e.g. [2022.12.07 Letter to Regulators re Banking System Crypto Exposure - updated.pdf \(senate.gov\)](https://www.senate.gov/imo/media/doc/letter/2022/12/07/2022-12-07-Letter-to-Regulators-re-Banking-System-Crypto-Exposure-updated.pdf).

5 See e.g. <https://www.bain.com/insights/web3-experiments-start-to-take-hold-in-banking/>; <https://www.forbes.com/sites/mariagraciasantillanalinaires/2022/10/03/banks-drawn-to-web3-technology-but-restrained-by-lack-of-rules/amp/>; <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/web-3-0-promises-big-changes-in-financial-sector-if-regulators-are-on-board-67587489>.

ty, and in particular software, can resolve numerous legal complications at a later date.⁶ Lawsuits involving intellectual property or other ownership rights may be inevitable but certain actions may reduce the number and scope.⁷ Activity that is illegal or inappropriate in the real world is unlikely to be sanctioned in a metaverse.⁸ And the list goes on.

History provides us with some guidance as to how these laws and regulations will be evolve in Web3. While Dr. Gavin Wood, the founder of Web3 Foundation, is credited with coining the term Web 3.0 in 2014,⁹ a number of predicate features can be found in earlier innovations. One of the most innovative was Second Life, considered the world's first metaverse. It was launched in 2003 by Linden Labs, as a virtual game that had its own currency to support a robust market economy in which users created their own content, operated real world and virtual businesses, generated tangible revenue and bought and sold virtual real estate and a variety of goods and services.¹⁰ A currency exchange provided convertibility of Linden Dollars, its "native" currency, to USD and other fiat currencies.

For a number of major corporations Second Life presented the testing ground for what was their first experiment in conducting business in a metaverse. These experiences provide a rich tapestry of what others launching metaverses likely will face, including intellectual property challenges arising out of user generated content. Second Life also established Tilia, a fully licensed and regulated money transmitter to support its business activities and those of other virtual gaming companies.¹¹

The process of understanding the application of and adapting existing laws and regulations to blockchain-based technologies has been underway from almost the day Satoshi Nakamoto released Bitcoin White Paper in 2008.¹² Since then, the implications of a number of legal issues associated Web3, including those raised by smart contracts and non-fungible tokens ("NFT"), have been analyzed by the crypto community and beyond. They have also been debated at both the federal and state levels of government

(and in some international arenas), in legislatures, regulatory agencies and the courts. A not insubstantial collection of law, regulations and precedence has been identified in this process as applying in part or whole to either Web3 or its component parts.

These laws include state money transmitter licensing and similar laws, securities laws, the federal Bank Secrecy Act that applies to certain types of entities engage in certain types of business activities, federal and state consumer protection laws, federal and state criminal laws prohibiting money laundering and terrorist financing and sanctions laws. This list is only partial and doesn't address a host of laws that are being retrofitted or enacted to address specific issues that arise as the result of the use of cryptocurrencies.

“For a number of major corporations Second Life presented the testing ground for what was their first experiment in conducting business in a metaverse

Although there are questions and gaps, developers – and anyone else – experimenting with and implementing Web3 strategies ignore at their own risk the myriad laws and regulations that apply, especially when two parties interact financially. In a centralized business model, the person – business or individual – controlling the operations is typically responsible for complying with these laws and regulations. In a decentralized environment where one person wants to conduct a financial transaction directly with another person, the burden for compliance with these laws and regulations shifts to the persons engaging in that transaction. The lack of an intermediary to assume responsibility for compliance

6 [Web3 Foundation Announces Polkadot Blockchain's Native Token \(DOT\) Has Morphed and Is Software, Not a Security | Web3 Foundation](#) (November 10, 2022).

7 See e.g. <https://www.coindesk.com/consensus-magazine/2023/01/27/better-policy-can-turn-nfts-into-an-intellectual-property-power-house/>.

8 See e.g. <https://www.justice.gov/usao-sdfl/pr/cryptocurrency-purchases-child-pornography-send-miami-man-federal-prison-12-years> ; <https://www.justice.gov/usao-edny/pr/founder-and-majority-owner-bitlato-cryptocurrency-exchange-charged-unlicensed-money>.

9 [What Is Web3, anyway? | WIRED](#) (November 28, 2021).

10 https://wiki.secondlife.com/wiki/History_of_Second_Life; <https://www.makeuseof.com/what-is-second-life-history-metaverse/>; <https://www.theatlantic.com/magazine/archive/2017/12/second-life-leslie-jamison/544149/>.

11 <https://www.makeuseof.com/what-is-second-life-history-metaverse/>.

12 <https://bitcoin.org/bitcoin.pdf>.

doesn't mean the compliance is not expected. Instead, the parties directly involved in the transaction are responsible for compliance and can be liable for noncompliance. And the liability does may not end with the parties to the transaction but may extend to the developer or those that may assist in facilitating the transaction, even if it is just writing the code.

Despite the allure of using cryptocurrencies for Web3 transactions – the potential for anonymous or pseudonymous transactions and the speed of the transactions across borders – the legal and compliance risks associated with the use of crypto currencies in this new world should not be minimized. Prosecutions of criminal activity and violations of law involving cryptocurrencies has not been spared in the uptick of sanctions enforcement especially against the backdrop of a major international conflict, the on-going siege of ransomware attacks, never-ceasing drug trafficking and an escalating focus on human trafficking, among other criminal activity.

U.S. sanctions laws apply to all U.S. persons, including any person resident in the U.S. and any U.S. citizen regardless of where they reside. The federal money laundering criminal statutes impose significant financial penalties and imprisonment of up to 20 years on “whoever” conducts or attempts to conduct a financial transaction that the person knows involves the proceeds of any one or more of 200 “specified unlawful activity” with the intent of carrying on the specified unlawful activity or conceal or disguise the nature, location, source, ownership or control of the proceeds, among other things.¹³ Similar statute prohibits providing material support terrorist activities,¹⁴ and both sets of statutes can be the basis for prosecuting those that aid and abet or are willfully blind to others engaging in such activities.¹⁵

“U.S. sanctions laws apply to all U.S. persons, including any person resident in the U.S. and any U.S. citizen regardless of where they reside

Moreover, the failure to register as a transmitter of money (money services business) or to seek the necessary state license if either or both is required is also a violation of a criminal statute and can result in monetary penalties and imprisonment of up to 5 years.¹⁶ Compliance with the regulations promulgated by the Financial Crimes Enforcement Network (“FinCEN”) to implement the Bank Secrecy Act requires another mindset that encompasses filing certain reports and creating additional transaction reports as well as instituting a regime for conducting customer due diligence (aka “KYC” or know your customer) and monitoring for suspicious activity.¹⁷ If the business model requires classification as a different type of regulated entity and compliance with other sections of the FinCEN regulations, certain due diligence and reporting requirements may differ and may in fact be more stringent.¹⁸ These requirements also apply from the first day the business is initiated and failure to comply can result in expensive regulatory intervention and fines.¹⁹

Of particular note has been the coordinated efforts of law enforcement, the national security community and regulators, domestically and foreign, to address the use of digital assets, including cryptocurrencies other tokens in money laundering, terrorist financing and other economic crimes as well as circumventing sanctions laws.²⁰ The core principles of Web3 as described by the Ethereum Foundation in acknowledging that “it’s challenging to provide a rigid definition of what Web3 is” highlight the reasons why Web3 is attracting such attention – decentralized, permissionless, trustless and has “native payments.”²¹ Decentralized means

13 18 U.S.C. 1956.

14 18 U.S.C. Sections 2339A, 2339B, 2339C.

15 See <https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance> ; <https://www.state.gov/anti-money-laundering-and-counter-ing-the-financing-of-terrorism/>.

16 18 U.S.C 1960.

17 See 31 CFR Chapter X.

18 <https://www.cftc.gov/PressRoom/PressReleases/8433-21> (CFTC imposes a \$1.25 million penalty against Kraken, Release No. 8433-21, 9/28/2021).

19 See https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202301041.

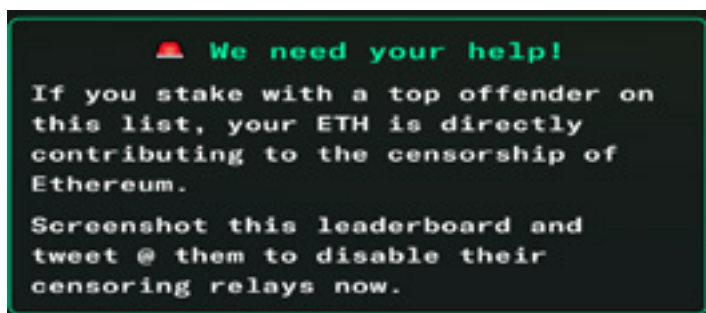
20 See <https://www.justice.gov/usao-edny/pr/founder-and-majority-owner-bitzlato-cryptocurrency-exchange-charged-unlicensed-money>; <https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance>.

21 [What is Web3 and why is it important? | ethereum.org](https://www.ethereum.org/en/what-is-web3).

that “instead of large swathes of the internet controlled and owned by centralized entities, ownership gets distributed amongst its builders and users.” Permissionless means “everyone has equal access to participate in Web3, and no one gets excluded.” Web3 is trustless because it “operates using incentives and economic mechanisms instead of relying on trusted third parties.” Last but certainly not least, the fact that Web3 uses native payments means that “instead of relying on the outdated infrastructure of banks and payment processors” Web3 “uses cryptocurrency for spending and sending money online.”

Each one of the core principles raises legal considerations with respect to AML/CTF and sanctions laws. Without centralized control, who will assume the responsibility for compliance with these laws. If truly decentralized, will each person be responsible for the required compliance. Is this a burden that each individual and businesses can assume? Regulated financial institutions, with significant resources allocated to compliance, often have difficulty staffing up sufficiently and with the right expertise to address these responsibilities.

The concept of permissionless – where everyone has access to participate in Web3, and no one gets excluded – is a potential red flag for sanctions violations. How does one comply with the prohibitions imposed on doing business with certain persons, especially if there is anonymity or pseudonymity is encouraged? Crypto exchanges have been on the radar screen of Office of Foreign Assets Control (“OFAC”) for several years and each action taken against such firms and others, especially companies conducting activities on the internet should be studied.²² [20220103_abnb.pdf \(treasury.gov\)](#) Tornado Cash raised a number of questions, including the possible complicity of those writing the code.²³ Noncompliance with sanctions rules has been openly encouraged in the wake of the action by the on one website that publishes real time data on entities exercising “censorship”²⁴



Consumer Protection will emerge. Consumer protection is another issue that cannot be ignored, in part because regulators have long memories and while crypto assets have not been at the top of the agenda of the Consumer Financial Protection Bureau and the Federal Trade Commission in recent years, as their focuses change, compliance shortcomings of the past may not be overlooked.²⁵

Bright spots ahead. In discussing one of the emerging use cases of Web3 – loyalty programs – Josh Rosenblatt aptly summed up the fact that current law applies to this use case in Web3 and underscores the importance of leveraging such laws and regulations and minimizing the need for new legislation and contrasts this use case with other Web3 use cases that may present greater challenges to lawmakers.²⁶

The entire industry will benefit if regulators and the public can think about crypto through the lens of Web3 loyalty programs, as regulatory frameworks already exist. Loyalty programs operate within well-established laws and regulations: consumer protection and privacy standards being among them. There are fewer open questions and less need for new legislation to govern Web3 loyalty programs.

Web3 loyalty programs are “nonthreatening.” Unlike other crypto use cases such as decentralized finance (“DeFi”), Web3 loyalty programs do not threaten the power of the state or traditional financial systems. It is very hard to financially harm consumers with a loyalty program. This makes them more politically palatable and easier to regulate.

Anticipating the future. As we look ahead to how laws and regulations affecting Web3 will evolve, especially as a result of lessons learned from the FTX debacle, the collapse of the defi lending sector and multiple hacks among other events, a clearer path for regulation may emerge. Without a doubt, the national security and criminal risks associated with Web3 will be a predominant concern for the indefinite future but risks well beyond these and ongoing intellectual property issues– will be looked at more closely and on a more systemic basis. But the core principles of Web3 as set out by the Ethereum Foundation – decentralized, permissionless, trustless and reliant on native currencies – ensure that that this path is not likely to be straight or easy to follow. As noted at the outset, this process requires the engagement of state-holders from all corners of the Web3 and massive educational efforts to ensure the trek through this new frontier is one that all can endure, and even enjoy! ■

22 See e.g. [20221128_kraken.pdf \(treasury.gov\)](#); [20221011_bittrex.pdf \(treasury.gov\)](#); [20220930_tango_card.pdf \(treasury.gov\)](#); [20220103_abnb.pdf \(treasury.gov\)](#).

23 [U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash | U.S. Department of the Treasury.](#)

24 [MEV Watch.](#)

25 [CFPB Director Chopra Statement on President Biden’s Digital Assets Executive Order | Consumer Financial Protection Bureau \(consumerfinance.gov\).](#)

26 [Web3 Loyalty Programs Are Catalyst for Good Crypto Policy and Adoption \(coindesk.com\).](#)

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit [competitionpolicyinternational.com](https://www.competitionpolicyinternational.com) today to see our available plans and join CPI's global community of antitrust experts.

