NEW YORK STATE BAR ASSOCIATION

Report and Recommendations of the New York State Bar Association **Task Force on Emerging Digital Finance and Currency**

June 2024

The views expressed in this report are solely those of the task force and do not represent those of the New York State Bar Association unless and until adopted by the House of Delegates.

Report and Recommendations of the New York State Bar Association Task Force on Emerging Digital Finance and Currency

June 2024

Members of the Task Force on Emerging Digital Finance and Currency

Task Force Co-Chairs

Jacqueline Jamin Drohan, Esq.
Matthew H. Feinberg, Esq.
Dana V. Syracuse, Esq.

Carlos Mauricio Mirandola, Esq., Vice Chair

Members

Joshua Lee Boehm, Esq.
Howard A. Fischer, Esq.
Felipe Hanszmann, Esq.
Nicholas G. Himonids, Esq.
Julie Houth, Esq.
Luca CM Melchionna, Esq.
Jeffrey D. Neuburger, Esq.
Rory Radding, Esq.
David Reiss, Esq.
David Schechtman, Esq.
Jason Schwartz, Esq.
Pablo Segarra, Esq.
A.F. David Steiner, Esq.
Yamicha Stephenson, Esq.
Margaret Strickler, Esq.
Romero Tapia, Esq.
Robin T. Williams, Esq.

Advisors

Stephen P. Younger, Esq.

Consultants

Marc Beckman
Nancy Chanin, Esq.

Student Members

Joseph Bizub
Dina Khedr
Tamara Szulc

Executive Committee Liaison

Sherry Levin Wallach, Esq.

NYSBA Staff Liaison

Hilary Jochmans

Administrative Support

Moe Whitcomb

Acknowledgements

The Task Force on Digital Finance & Currency would like to express its sincere gratitude to its student members Joe Bizub and Tamara Szulac for their dedication to its mission and work as well as their outstanding editorial assistance.

The work of the Task Force and its multiple continuing legal education programs including the development of Deep Dive into Web3 & the Metaverse, would not have been possible without the support and continued sponsorships from DMA United, DMA United CEO & President Marc Beckman, New York University's School of Professional Studies, NYU SPS Dean Angela Kamath, Crescite, Crescite Co-Founders Eddie Cullen, CEO & Karl P. Kill III, Chairman and Jurat.

Finally, the Task Force wishes to thank NYSBA Past President Stephen P. Younger, Nixon Peabody for his support and guidance.

The Report of the Task Force on Digital Finance & Currency

Introduction

Web 3

Web3 stands as a revolutionary milestone in the internet's evolution, transitioning from the centralized frameworks of Web1 and Web2 towards a decentralized architecture. This shift, underpinned by blockchain technology, introduces a new paradigm where decentralized applications (dApps) and smart contracts facilitate a digital experience centered around user empowerment and autonomy.

The journey from Web1 to Web3 encapsulates a remarkable evolution in how content is created, shared, and controlled. Web1, the internet's nascent phase, was primarily read-only, offering static content with limited interaction. Web2 marked a significant leap forward, characterized by social media, e-commerce, and user-generated content, leading to the rise of digital conglomerates that amassed considerable control over data and user interactions.

Web3 emerges as a paradigm shift, emphasizing decentralization and user sovereignty, enabled by blockchain technology. This era challenges the centralized models of Web2, proposing a web where users have unprecedented control over their data, identity, and digital assets. Blockchain's role in this transition is pivotal, providing the infrastructure for secure, transparent, and intermediary-free transactions.

Blockchain: The Catalyst for Decentralization

Blockchain technology is at the heart of Web3, disrupting traditional digital commerce and data management practices. By enabling decentralized transactions, blockchain technology diminishes the need for central authorities or intermediaries, facilitating a transparent and efficient exchange of digital assets. This technology is not limited to cryptocurrencies but extends to a wide range of applications across finance, healthcare, the arts, and more, fostering innovation and new business models.

The decentralized nature of blockchain presents a unique set of legal challenges and considerations. For those in the legal community, understanding the intricacies of blockchain technology is essential for navigating the legal landscape of digital assets, smart contracts, and the broader implications for intellectual property, data privacy, and commercial transactions.

Blockchain technology and digital currencies have captured the imagination of the financial world, as well as many other industries, by offering a new way to conduct transactions and store data securely. At the core of these innovations lies the

blockchain, a decentralized digital ledger that records transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks.

Blockchain is essentially a distributed database that maintains a continuously growing list of records, called blocks, which are linked and secured using cryptographic principles. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. This design allows for secure and transparent transactions that are resistant to fraud and tampering.

"Blockchain's heart is a peer-to-peer network, instead of a central server. Blockchain's brain is a consensus algorithm that syncs the peer-to-peer network at regular intervals. And Blockchain's lifeblood is an encrypted, linked log of data. Together, these three technologies yield a chronological, immutable ledger that is distributed across many participants. Because a Blockchain does not exist in one place, it offers two distinct advantages over a central server: both broader access and greater security."[1] In sum, blockchain technology is a decentralized ledger that maintains a tamper-proof record of transactions across a network of computers.

Digital currencies, also known as cryptocurrencies, are the most renowned application of blockchain technology. Bitcoin, introduced in 2009, is the first and most well-known cryptocurrency. Unlike traditional currencies, cryptocurrencies are not controlled by any central authority, such as a government or financial institution. Instead, they rely on a decentralized network of computers to manage and record transactions. This ensures that the currency is completely digital, and its creation and transactions are regulated by cryptography.

Implications for Digital Commerce and Data Ownership

The shift to Web3 has profound implications for digital commerce and data ownership, redefining the legal and commercial frameworks that govern digital interactions. In Web3, the ownership of digital assets and personal data shifts towards the user, challenging the traditional models of data control and monetization practiced by centralized platforms.

Since the early 2000s, digital currencies have continued to emerge and businesses supporting and promoting their use have continued to develop. Their rise and increased use worldwide have created a new market and purchase power. As with any currency, digital currencies have become increasingly an avenue for criminal

[1] Paul Embley and Di Graski, "When Might Blockchain Appear in Your Court?" National Center for State Courts, (2018) https://www.ncsc.org/__data/assets/pdf_file/0018/14913/blockchaininthecourts.pdf.

enterprise, but the technology behind them also provides new opportunities for growth, connectivity, and development.

For legal professionals, this shift necessitates a reevaluation of existing legal frameworks to accommodate the decentralized, blockchain-based model of Web3. Issues of jurisdiction, enforceability of smart contracts, intellectual property rights in a decentralized context, and compliance with data protection regulations become increasingly complex.

The decentralization inherent in Web3 raises questions about governance, dispute resolution, and the applicability of traditional legal mechanisms in a distributed digital environment. We in the legal community must consider how legal principles apply in a landscape where transactions and interactions occur across a global, decentralized network without centralized oversight.

New York is a leader for the legal community and emerging technology in the United States. As is reported herein, several of the leading cases and regulatory frameworks are being litigated in New York Courts, by New York agencies and legislators. As such, it is imperative that the New York State Bar Association continue its leadership of the legal community as these technologies continue to evolve and impact the law.

Executive Summary

The NYSBA Task Force on Emerging Digital Finance and Currency ("Task Force") was formed by Immediate NYSBA Past President Sherry Levin Wallach. The mission statement of the Task Force is: "to study and evaluate the legal issues and questions surrounding the expansion and regulation of the digital finance and digital currency industries in New York State. This review may include the development of best practices for attorneys representing clients on matters in these areas and the proposal of law and policy recommendations to the relevant regulatory bodies in this evolving field."

The Task Force issued its interim report and recommendations, which were approved by the House of Delegates in April 2023.[2] The instant report constitutes the Final Report ("Final Report") and recommendations of the Task Force. The Final Report details the regulatory landscape, possible ways to navigate Web3 businesses through a sandbox approach, Federal Income Tax considerations regarding digital assets, intellectual property considerations in Web3, navigating the nexus of criminal justice and emerging technologies, as well as ethics and education.

Blockchain's part in this evolution is pivotal, providing the infrastructure for secure, transparent, and intermediary-free transactions. Blockchain technology is at the heart of Web3, including emerging digital finance and currencies, disturbing customary digital commerce and data management practices. By empowering decentralized transactions, blockchain technology reduces the need for central authorities or intermediaries, facilitating a transparent and efficient exchange of digital assets. This technology is not limited to cryptocurrencies but extends to a wide range of applications across finance, healthcare, the arts, and more, fostering innovation and new business models.

Of critical importance, as discussed in the Final Report, the decentralized nature of blockchain presents a unique set of legal challenges and considerations. For those in the legal community, understanding the intricacies of blockchain technology is essential for navigating the legal landscape of digital assets, consumer protection, smart contracts, and the broader implications for intellectual property, data privacy, and commercial transactions. The shift to Web3 has profound implications for digital commerce and data ownership, redefining the legal and commercial frameworks that govern digital interactions. In Web3, the ownership of digital assets and personal data

[2] https://nysba.org/app/uploads/2022/03/final-no-changes-Task-Force-on-Emerging-Digital-Finance-and-Currency-April-2023-1.pdf

shifts towards the user, challenging the traditional models of data control and monetization practiced by centralized platforms.

For legal professionals, the shift to Web3 requires a re-evaluation of existing legal frameworks to accommodate its decentralized, blockchain-based model, along with digital finance and currencies. This evolution introduces complexities regarding jurisdiction, enforceability of smart contracts, intellectual property rights in a decentralized context, and compliance with data protection regulations become increasingly complex. Moreover, as the Final Report highlights, the decentralization inherent in Web3 raises questions about governance, dispute resolution, and the applicability of traditional legal mechanisms in a distributed digital environment. As emphasized in the Final Report's recommendations, we in the legal community, especially those of us practicing law in New York, must consider how legal principles apply in a landscape where transactions and interactions occur across a global, decentralized network, absent centralized oversight.

This technology and its applications are evolving more rapidly than ever before. As usage increases, the legal profession must continue to address new considerations and issues. These technologies offer opportunities for improved client representation, enhanced data security and sharing, and increased efficiency. Simultaneously, questions and concerns continue to be raised in all aspects of legal practice. Therefore, it is essential to continue educating the legal profession and explore ways to leverage this technology to enhance legal practice and client representation. This report gives an overview of our past progress, our current trajectory, and identifies both opportunities and challenges. The following recommendations aim to guide the legal community on this journey.

Recommendation of the Task Force

A. *Create an Integrated Committee on Technology*:

This committee would combine the Task Force on Emerging Digital Finance & Currency, Committee on Law & Technology, and the Task Force on Artificial Intelligence and create a centralized group to continue to explore and study issues.

B. *Dispute Resolution and Enforcement:*

Developing new legal frameworks and dispute resolution mechanisms that can accommodate the decentralized nature of blockchain transactions is crucial. This might include specialized courts or arbitration panels familiar with blockchain technology and real property law.

C. *Use Emerging Technologies to Enhance Member Benefits:*

Initiate a request for proposals (RFP) from companies or organizations with expertise in emerging technology to integrate these technologies with those currently in use to increase member benefit and support.

Articles 1, 2 & 3: Recommendations Regulatory Landscape

D. *Enact Clear Federal Legislation on Digital Assets:*

Congress should prioritize the enactment of clear, comprehensive federal legislation that specifically addresses the classification, taxation, and regulatory oversight of digital assets. This legislation should provide a definitive framework for determining when a digital asset is considered a security, commodity, or a new, distinct asset class. Additionally, the legislation should address the use of digital assets in various sectors, including finance, healthcare, and supply chain management.

E. *Improve and Enhance Appropriate Regulatory Frameworks and Oversight:*

To address the regulatory ambiguity and jurisdictional disputes, proposed legislation should aim to clearly define which agencies are responsible for regulating different aspects of the industry. This includes establishing more objective criteria for when and how crypto assets should move between regulatory regimes. By its nature, this is a global financial service. We need national oversight with state licensing like the rest of the financial and insurance industry.

F. *Establish a Regulatory Sandbox for Digital Assets:*

Regulatory sandboxes are innovative frameworks allowing businesses to test novel products and services in a controlled environment under regulatory supervision. This concept, drawing from the iterative testing approach commonly used in the tech industry, offers valuable insights for both regulators and innovators. It ensures that regulatory frameworks can adapt to technological advances while safeguarding consumer interests and maintaining financial stability.

The United States Federal and State governments should create a regulatory sandbox that allows companies to develop and test innovative digital asset products and services within a safe harbor, under the guidance and supervision of regulators. The sandbox would offer a period of regulatory relief, during which companies can receive input from regulators on the development and alignment of their business models with legal and regulatory requirements.

G. *Foster Innovation and Collaboration:*

Advocate for regulatory bodies to foster innovation in the digital asset space by establishing appropriate regulatory sandboxes or pilot programs. These initiatives should allow for experimentation with digital asset technologies under a relaxed

regulatory framework, subject to oversight and review. Promote collaboration between regulators, academia, and the private sector to research and develop best practices for the use and regulation of digital assets. Additionally, support educational initiatives to enhance the understanding of digital assets and blockchain technology among regulators, law enforcement, and the general public.

H. *Taxation of Digital Assets and Currencies:*

The IRS has not provided taxpayers with sufficient opportunities to engage discussions on the appropriate treatment of block rewards. As a result, there remains significant uncertainty around ancillary questions. We recommend that NYSBA advocate for clear guidelines and rules regarding the taxation of digital assets and currencies.

Article 4: Intellectual Property Considerations in Web3

I. *International Cooperation and Harmonization:*

Given the global nature of Web3, there is a pressing need for international cooperation and harmonization of trademark laws to tackle the challenges associated with branding digital assets. Developing standardized protocols for the registration, recognition, and enforcement of trademarks across borders could help mitigate some of the jurisdictional challenges posed by Web3.

J. Legal Recognition of Digital Titles:

Laws should recognize digital titles and registrations on a blockchain as legally valid and equivalent to traditional paper titles. This involves ensuring that digital records meet all legal requirements for real property transactions, including evidence of ownership, encumbrances, and liens.

Implementing a hybrid system that maintains traditional title registration mechanisms while integrating blockchain technology could offer a transitional solution. This approach would leverage blockchain's efficiency and security while retaining the legal framework's established protections and recognitions.

Article 5: Navigating the Nexus of Emerging Technologies and Criminal Justice: Challenges and Opportunities in the Age of Digital Currencies and Assets

K. *Continue to explore the implementation of the Use of Blockchain Technology in the Criminal Justice System to Enhance Efficiency and Access to Justice:*

Blockchain can be used to provide more secure access and more efficient storage and transfer of data such as for record keeping, maintaining police disciplinary data systems, service of process and to create uniform statewide pre-trial data collection. This will increase the integrity of the system and decrease wrongful convictions and unnecessary or prolonged incarceration.

L. *Consideration Should be Given to the Use of Digital Currency in Certain Aspects of the Criminal Justice System:*

Digital currencies are being used worldwide to bank the unbankable. Further, by their very nature, they provide a secure manner for the transfer of funds while increasing accessibility. We recommend the use of Digital Currency be explored for bail, as a source of currencies for incarcerated people, restitution and for payment of fines and court fees.

M. *Importance of Cross-Jurisdictional Cooperation & Collaboration:*

It is essential that the legal community continue to cooperate and develop cross-border relationships and collaborations to protect the communities and clients as well as provide the best opportunities for weeding out bad actors.

Article 6: Recommendations Ethics & Education

N. *Ethical Clarity Regarding Fee Arrangement Concerning Cryptocurrency:*

To avoid a potential ethical quagmire, when presented with a fee arrangement concerning cryptocurrency, the attorney should review the entire RPC, especially sections 1.5(a) and 1.8(a) to determine applicability and always act cautiously. Furthermore, whether RPC 1.8(a) could be reasonably implicated is immaterial, as any attorney holding cryptocurrency as a type of payment in advance should disclose the possible ethical issues implicated under RPC 1.8(a) in writing and further evaluate whether any other rules might be implicated. Being that an attorney is a fiduciary, the absence of such a writing, in the event there is an unexpected ethical quagmire, could result in an adverse inference regarding the attorney's conduct.

A way to avoid the pitfalls associated with an RPC 1.8(a) dilemma is to liquidate any cryptocurrency into fiat immediately upon receipt of payment. This is likely the more prudent approach to take, especially for an attorney not as familiar with cryptocurrency and until the tech is more universally adopted. Unless an attorney has the means necessary to adhere to the rules, better safe than sorry. Importantly, NYSBA should provide guidance as to whether attorneys can accept crypto as advanced payment for legal services.

O. *Continued Engagement in Law School Education:*

While law schools are increasingly doing their part to attempt to provide law students with opportunities to learn about these emerging technologies at the foundational level, the present bar must stay abreast of the changing technology. NYSBA should continue to engage with these programs.

P. *Best Practices:*

Develop best practices for attorneys engaging in the digital assets & crypto currency space. Attorneys must be diligent in following the guidelines of the commentary to the Code of Ethics and ensure their actions do not violate any cannons or criminal laws. Attorneys must also be diligent in advising their clients on the importance of KYC to prevent unintended consequences.

Article 1: The Regulatory Landscape

SECTION 1: SEC's Approach to Token Classification

The landscape of digital asset regulation in the United States has been significantly shaped by the Securities and Exchange Commission's (SEC) enforcement actions. The decisions from the courts have been one source of guidance. However, the landscape remains uncertain. The SEC's first notable foray into the cryptocurrency space occurred in July 2013 with *SEC v. Shavers*, where the court held that Bitcoin could be considered a form of money, and thus investments denominated in Bitcoin could be considered securities under the *Howey* test.[3]

This set the stage for the SEC's evolving approach to token classification, which became more defined with the release of *The DAO Report* in July 2017. The report marked the first instance where the SEC explicitly categorized a token as a security.[4] The DAO, a Decentralized Autonomous Organization, offered its own tokens for purchase using Ether, with the promise of funding projects and providing returns to token holders. The SEC's application of the *Howey* test to The DAO's offering underscored the agency's view that tokens representing investments in ventures expecting profits from the efforts of others could be considered securities.[5]

The DAO Report laid the groundwork for the SEC's case-by-case approach to evaluating tokens, emphasizing that the determination of whether a token is a security depends on the specific facts and circumstances of each offering.[6] This approach has been reiterated in subsequent enforcement actions and public statements, highlighting the need for a nuanced analysis of token offerings to assess compliance with federal securities laws.

The DAO Report targeted the Decentralized Autonomous Organization (the "DAO"), an organization offering its own tokens for purchase using the Ethereum Blockchain token, Ether. The tokens represented interests in the DAO platform, and its organizers would invest in projects that received a majority vote from DAO token

[3] *SEC v. Shavers*, No. 4:13-CV-416-17 (E.D. Tex. Aug. 6, 2013), adhered to on reconsideration, No. 4:13-CV-416 (E.D. Tex. Aug. 26, 2014).
[4] SEC, Report of Investigation Pursuant to Section 21(A) of the Securities Exchange Act of 1934: The "DAO Report", securities act release no. 81207 (July 25, 2017) (applying the traditional securities *Howey* Test to conclude the DAO Token was a security).
[5] *Id.* at 10.
[6] *See* In the Matter of Munchee Inc., SEC Release No. 33-10445 (Dec. 11, 2017) (cease and desist order); AirFox, Paragon, Crypto Asset Management, TokenLot, and EtherDelta's founder. Division of Corporation Finance, Division of Investment Management, and Division of Trading and Markets. "Statement on Digital Asset Securities Issuance and Trading." Nov. 16, 2018. SEC.

holders. Created by Slock.it, the platform was marketed as a "for-profit entity whose objective was to fund projects in exchange for a return on investment."[7] The DAO, despite a massive fundraise over $150 million was not registered in any sovereign jurisdiction. Nor did the DAO have a board of directors, a CEO, or a management team. The rationale behind the crowdfunding was the creation of new software applications, but before the venture took flight, it was hit with a cyber-attack draining 1/3rd of its funds.

The SEC investigated the DAO in connection with the offering's potential applicability to federal securities laws and whether the tokens constituted securities.[8] Applying the *Howey* test, the SEC focused on the fact that Slock.it used "various promotional materials disseminated by Slock.it and its cofounders informed investors that [t]he DAO was a for-profit entity whose objective was to fund 12 projects in exchange for a return on investment."[9] Additionally, the DAO token satisfied the expectation of profits prong because "the DAO's investors relied on the managerial and entrepreneurial efforts of Slock.it and its co-founders, and the DAO's Curators, to manage the DAO and put forth project proposals that could generate profits for the DAO's investors."[10] Lastly, while DAO token holders had certain voting rights, this did not grant them "control over the enterprise," and thus the fourth prong of the *Howey* test was also satisfied.[11]

Overall, *The DAO Report* stated that U.S. federal securities laws "may apply" to "virtual tokens" and confirmed the analysis would depend on an application of the *Howey* test to the specific "facts and circumstances" of each token sale.[12] Applying this guidance, *The DAO Report* concluded that the DAO token in question constituted a security for at least three reasons: (1) purchasers jointly contributed funds to invest in projects; (2) token holders obtained the right to vote on where to invest; and (3) holders received pro rata dividend payments from each project's profits.[13]

However, while seminal in nature, *The DAO Report* cannot be read to suggest all digital assets are subject to federal securities laws. Rather, the SEC has stated on several occasions that certain tokens, *e.g.*, Bitcoin is not security, but the SEC officials have waivered regarding Ether.[14] *The DAO Report* solidified the notion that the SEC has authority to regulate cryptocurrencies and that each token evaluation is on a case-

[7] *Id.*
[8] *Id.*
[9] *Id.* at 12.
[10] *Id.*
[11] *Id.*
[12] *Id.* at 10.
[13] *Id.* at 17-18.
[14] William Hinman's Statements as the Director of the Division of Corporation Finance SEC. "Digital Asset Transactions: When Howey Met Gary (Plastic)." June 14, 2018. https://www.sec.gov/news/speech/speech-hinman-061418

by-case basis. In other words, no set token standard exists for whether one type of token is or is not a security but applying this precedent to token frameworks provides insight into compliance requirements, if any.

Since the *DAO Report*, the SEC has brought a number of enforcement actions targeting token-based projects. Several were brought by the SEC Cyber Asset and Cyber Unit (CACU), an entity formed to "focus the Enforcement Division's substantial cyber-related expertise on targeting cyber-related misconduct," including "[v]iolations involving distributed ledger technology and initial coin offerings." As the SEC noted in a court filing, certain offerings are effectively "old-fashioned fraud dressed in a new-fashioned label."[15]

Overall, these cases show the SEC's intention to combat fraud and bad actors as applied to cryptocurrencies and token offerings. In fact, the agency issued several alerts to warn potential investors about the risks involved in participating in token offerings (also referred to as Initial Coin Offerings ("ICOs")).[16] Therefore, a specific analysis of the facts of the token is necessary as well as how and when information was presented to those who receive tokens.

The Howey Test

Section 2(a)(1) of the Securities Act of 1933 defines "securities" as: "any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement … investment contract … or, in general, any interest or instrument commonly known as a 'security', or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing."[17] A broad definition, Section 2(a)(1) carries significant precedent regarding statutory interpretation.

The seminal Supreme Court case for interpreting Section 2(a)(1) is *SEC v. Howey*,[18] which created the test, *i.e.*, the *Howey* test, used to determine whether an

[15] *See e.g.*, *U.S. v. Zaslavskiy*, No. 1:17-cr-00647, slip op., 2018 WL 4346339 (E.D.N.Y. Sept. 11, 2018) (Judge Raymond Dearie of the Eastern District of New York upheld a criminal indictment for securities fraud involving the sales of cryptocurrency tokens in an ICO); *Commodity Futures Trading Commission v. McDonnell*, 287 F. Supp. 3d 213 (E.D.N.Y. 2018) (determining that fraudulent ICOs can be subject to enforcement proceedings under the antifraud provisions of the Commodities Exchange Act).
[16] SEC. "Spotlight on Initial Coin Offerings and Digital Assets." https://www.sec.gov/spotlight-initial-coin-offerings-and-digital-assets
[17] *See* 15 U.S.C. § 77b.
[18] 328 U.S. 293 (1946).

instrument meets the definition of a "security" under the Securities Act.[19] In *Howey*, the Court held that units of a citrus grove, coupled with a contract for serving the grove, was an investment contract.[20] The defendants offered buyers the option of leasing any purchased land back to the defendants, who would then tend to the land, and harvest, pool, and market the citrus.[21] The SEC sued defendants over these transactions, claiming they broke the law by not filing a securities registration statement.[22] The Supreme Court, in issuing its decision finding the defendants' leaseback agreement is a form of security, developed a landmark test for determining whether certain transactions are investment contracts.

The Court in *Howey* specifically defined the term "investment contract" within the definition of a "security," noting it has been used to classify instruments that are of a "more variable character" that may be considered a form of "contract, transaction, or scheme whereby an investor lays out money in a way intended to secure income or profit from its employment."[23] The Supreme Court has recognized lower courts subsequently have required only an expectation of profits from the efforts of others, rather than solely from the efforts of others when determining whether a financial instrument is a security. [24]

The *Howey* test is divided into four prongs:

> An investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person [1] invests his [or her] money in [2] a common enterprise and is led to [3] expect profits [4] solely from the efforts of the promoter or a third party, [excluded factors] it being immaterial whether the

[19] Indeed, the Court has referred to the test established by *Howey* for determining whether an instrument is a security as, "in shorthand form, [embodying] the essential attributes that run through all of the Court's decision defining a security." *See United Housing Found., Inc. v. Forman*, 421 U.S. 837, 852 (1975). However, the Court subsequently emphasized that this statement was meant to apply only in the context of determining whether an instrument is an investment contract. *See Landreth Timber Co. v. Landreth*, 471 U.S. 681, 691 n.5 (1985).
[20] 328 U.S. at 239.
[21] *Id.*
[22] *Id.* at 298.
[23] *Id.* at 239, 298-99. In *Howey*, the Court stated that "[s]uch a definition necessarily underlies" the Court's earlier decision in *SEC v. C.M. Joiner Leasing Corp.*, 320 U.S. 344 (1943). In *Joiner*, the Court held that the offer of oil and gas leaseholders, which would be drilled by the offeror for the buyer, was the offer of a security. In rejecting the claim that these rights were strictly leasehold interests, the Court foreshadowed the later opinion in *Howey*. The Court also has relied on the *Howey* definition of the term "investment contract" in subsequent decisions, such as when it held that a variable annuity contract is a security (*see SEC v. Variable Annuity Life Ins. Co. of America*, 359 U.S. 65, 72 n. 13 (1959)) and when it held that withdrawable capital shares in a state-chartered savings and loan association were securities rather than certificates of deposit (*see Tcherepnin v. Knight*, 389 U.S. 332, 338 (1967). *See also SEC v. United Benefit Life Ins. Co.*, 387 U.S. 202 (1967) (holding that the accumulation portion of a flexible fund variable annuity contract was an investment contract for purposes of the Securities Act).
[24] *Formando.*, 421 U.S. at 852 n.16.

> shares in the enterprise are evidenced by formal certificates or by nominal interests in the physical assets employed in the enterprise.[25]

In order to be considered a security, all four factors must be met. In other words, if an instrument does not satisfy the requirements of the *Howey* test, it is not an investment contract, and thus not a security.

For example, in *International Brotherhood of Teamsters v. Daniel*,[26] the Court held interests in a noncontributory, compulsory pension plan were not investment contracts because there was "no investment" of money and no expectation of profit from a common enterprise.[27] The Court also has held an investment contract is not present "when a purchaser is motivated by a desire to use or consume the item purchased."[28] In *United Housing Found., Inc. v. Forman*, the Court held, among other things, that shares in a nonprofit cooperative housing corporation were not investment contracts because "investors were attracted solely by the prospect of acquiring a place to live, and not by financial returns on their investments."[29]

Considering this precedent, U.S. Courts have interpreted the *Howey* test broadly, *e.g.*, an investment of money may include not only the provision of capital, assets and cash, but also goods, services or a promissory note.[30] Indeed, according to the Supreme Court, the *Howey* test "embodies a flexible rather than a static principle, one capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits."[31]

This consumer protection precedent provides a fact-specific application to ensure any interpretation does not go beyond not only the intended purpose of the *Howey* test but also the statutory language within the Securities Act. Overall, the test eschews classification based on formalities, such as offering stock certificates, or terminology, such as selling "shares" or "stock," in favor of a flexible test based on economic circumstances. As the *Tcherepnin v. Knight* opinion affirms, "in searching for the meaning and scope of the word 'security' . . . form should be disregarded for substance and the emphasis should be on economic reality."[32]

---

[25] 328 U.S. 299; *see also SEC v. Edwards*, 540 U.S. 389, 393 (2004) (reaffirming the *Howey* analysis); *see also Forman*, 421 U.S. at 852-53 (The "touchstone" of an investment contract "is the presence of an investment in a common venture premised on a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others.").
[26] 439 U.S. 551 (1979).
[27] *Id.* at 559-62.
[28] *See Forman*, 421 U.S. at 852-53.
[29] *Id.* at 853.
[30] *Howey*, *supra* note 6, at 299.
[31] *Id.*
[32] *Tcherepnin*, 389 U.S. at 336.

Generating tokens via a blockchain platform can generate a security and be characterized as taking "nominal interests in the physical assets employed in the enterprise."[33] Indeed, cryptocurrency technology has, assuredly, been utilized in certain circumstances as persuasive window-dressing in the marketing of Ponzi schemes, or to use the *Howey* Court's terms, "schemes devised by those who seek the use of the money of others on the promise of profits."[34] This is a reality of the industry, and certain regulatory actions regarding cryptocurrency projects are certainly justified.

However, each case requires a fact-specific application of precedent, and in circumstances where a Foundation sells tokens that contain immediate functionality for an online platform, Courts and administrative agencies would be hard-pressed to determine this type of token constitutes a security.

The general administrative precedent regarding categorizing cryptocurrencies as securities exists,[35] *e.g., The DAO Report*, the majority of interpretative guidance, starts with a determination of whether an investment exists. However, before diving into the administrative application, an understanding regarding traditional cryptocurrency categorization, for which there is scant precedent, in the securities context is not only needed, but at the forefront of the analysis.

SECTION 2: Virtual Currencies Under the U.S. Commodity Exchange Act – Mixed Signals

In October 2019, CFTC Chairman Heath Talbert stated "[i]t is my view as chairman of the CFTC that Ether is a commodity," said CFTC Chairman Heath Tarbert.[36] The Commission's intentions to regulate the sector were shortly followed by its ground-and record-breakingly rapid designation of an ETH-based CBOE exchange tradable futures contract, making ETH futures legal for trading in the US, even by retail investors.[37] Similarly, CFTC this week authorized a crypto trading firm to integrate its issuance, advisory and trading components, another first. His successor*, CFTC* Commissioner Dawn DeBerry Stump, stated as recently as August 2021 that "even if a digital asset is a commodity, it is not regulated by the CFTC. However: The CFTC does regulate derivatives on digital assets, just like it regulates other derivatives."[38]

---

[33] *Howey*, *supra* note 6, at 299.
[34] *Id.*
[35] The DAO Report, *supra* note 4.
[36] Paddy Baker, "CFTC Declares Ethereum's Ether a Commodity," Crypto Briefing (Oct. 10, 2019), https://cryptobriefing.com/eth-futures-commodity/.
[37] Cboe Digital, https://www.erisx.com/product/futures/, (last visited Apr. 14, 2024).
[38] Sam Cooling, "CFTC reminds SEC 'We regulate derivatives not digital assets,'" Yahoo! Finance, (Aug. 24, 2021), https://finance.yahoo.com/news/cftc-reminds-sec-regulate-derivatives-123215809.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAALjBrsXlw_ho4C_LCHiMQkYnb6_0h-

It should be noted that even under the tenure of CFTC Chairman Gensler, the commission largely argued to expand its jurisdiction over the sector, and to limit available exemptions. Subsequently, Gensler, as Chair of the SEC, has overseen that agency's efforts to instead classify most virtual currencies as securities and expand SEC oversight. In both cases, agency guidance has been persistently vague in the view of many legal practitioners.

What makes a Virtual Currency Fully Regulatable by the CFTC?

Two often overlooked but potentially applicable questions of federal law and regulation are: 1. When does a virtual asset constitute an exempt deliverable commodity contact under the U.S. Commodity Exchange Act (CEA), 7 U.S.C. § 2(c)(2)(D)? If it does not so qualify, it may constitute an illegal off-exchange futures contract. 2. When does it constitute a derivative? If the crypto contract constitutes an OTC derivative it is illegal to offer it to U.S. retail investors under the CEA. Even if offered to qualifying Eligible Contract Participants (7 U.S.C. § 1a(18)) the offering company may fall under Swap Dealer and/or Swap Execution Facility registration requirements. Unexpected results may occur here where an offering is an NDF or has optionality features, but also where linked to Smart Contract, or dealt on a platform with "closed system" architecture.

CFTC Jurisdiction

The 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act (''Dodd-Frank Act'') amended the Commodity Exchange Act (''CEA'') to, inter alia, add a new subparagraph, section 2(c)(2)(D) of the CEA entitled ''Retail Commodity Transactions.''[39] New section 2(c)(2)(D) makes subject to the CEA any agreement, contract, or transaction in any commodity that is entered into with, or offered to a non-eligible contract participant or non- eligible commercial entity on a leveraged or margined basis, or financed by the offeror, the counterparty, or a person acting in concert with the offeror or counterparty.[40] This section excepts certain transactions from its application. In particular, CEA section 2(c)(2)(D)(ii)(III)(aa) provides exceptions for a contract of sale that results in actual delivery within 28 days or such other longer period as the Commission may determine by rule or regulation.[41]

YsAAK7G0Y9tPUes31UGI6tOnqkP7ifPUc80gugovHIkpxij6jQID0qjmi5QVQN3nv_RQrLfjXgFuUYZJWr7cs4gWsaj_xZegkbFOXSoUidMXdt89Z45j-RQdM6D5FB-e48o2RDDEP7TF5w.

[39] Commodity Futures Trading Commission, "Dodd-Frank Act"

[40] *Id.* https://www.cftc.gov/sites/default/files/idc/groups/public/@swaps/documents/file/hr4173_enrolledbill.pdf

[41] *Id.*

Section 2(c)(2)(D) of the CEA provides the CFTC with direct oversight and authority over "retail commodity transactions" – defined as agreements, contracts or transactions in any commodity that are entered into with or offered to retail market participants on a leveraged or margined basis, or financed by the offeror, the counterparty or a person acting in concert with the offeror or counterparty on a similar basis. Such a transaction is subject to the CEA "as if" it were a commodity future.[42] This statute contains an exception for contracts of sale that result in "actual delivery" within 28 days from the date of the transaction. The Commission by public comment, enforcement posture and civil advocacy has taken the position since 2015 that virtual currencies constitute "commodity transactions" for purposes of the CEA (including section 2(c)(2)(D) thereof).[43]

Prior Commission Interpretations re CEA §2(c)(2)(D)

On December 14, 2011, the Commission proposed an interpretation of CEA section 2(c)(2)(D) and the meaning of "actual delivery" as used therein and solicited public comment.[44] The Commission clarified its interpretation on the basis of these comments by Federal Register Release on August 23, 2013 (the "Clarified Interpretation"). [45] The Clarified Interpretation stated (quoting the original Interpretation) that ''in determining whether actual delivery has occurred within 28 days, the Commission will employ a functional approach and examine how the agreement, contract, or transaction is marketed, managed, and performed, instead of relying solely on language used by the parties in the agreement, contract, or transaction.''[46] It further stated that the Commission would consider as relevant factors "[o]wnership, possession, title, and physical location of the commodity purchased or sold, both before and after execution of the agreement, contract, or transaction; the nature of the relationship between the buyer, seller, and possessor of the commodity purchased or sold; and the manner in which the purchase or sale is recorded and completed."[47] While the "Clarified Interpretation" provided a list of examples which indicated that actual delivery required the transfer of title and possession to the purchaser or the purchaser's depository, it stated that book entries in which a purchase is rolled or offset do not constitute actual delivery.

---

[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] https://www.federalregister.gov/documents/2013/08/23/2013-20617/retail-commodity-transactions-under-commodity-exchange-act
[46] *Id.*
[47] *Id.*

March 24, 2020, Final Interpretation

On March 24, 2020, the CFTC issued its final interpretive guidance (the "Final Interpretation") on the meaning of "actual delivery" in the context of § 2(c)(2)(D) retail commodity transactions involving virtual currencies.[48] The Interpretation states that "actual delivery" of retail virtual currency transactions occurs when: 1. a retail person secures: (i) possession and control of the entire quantity of the commodity, whether it was purchased on margin, or using leverage, or any other financing arrangement, and (ii) the ability to use the entire quantity of the commodity freely in commerce (away from any particular execution venue) no later than 28 days from the date of the transaction and at all times thereafter; and 2. the offeror or counterparty seller do not retain any interest in, legal right, or control over any of the commodity purchased on margin, leverage, or other financing arrangement at the expiration of 28 days from the date of the transaction.[49]

While the Final Interpretation was intended by the CFTC to provide greater certainty regarding the scope of the § 2(c)(2)(D) exemption, and contains a number of examples for illustrative purposes, it in fact provided little bright line guidance beyond the CFTC's original public positions and enforcement posture. The Final Interpretation itself notes that CFTC will continue to "employ a functional approach" and "assess all relevant factors that inform an actual determination."[50]

Of equal relevance is CFTC's failure to resolve or address a number of public comments received from industry participants in the Final Interpretation. The proposed "possession and control" and "free use in commerce" requirements might act to wholly vitiate the exception for margined OTC principal-to-principal commodity transactions intended by Congress. If these standards are applied too rigorously, they would preclude any form of hypothecation or enforceable security interest in the assets financed, effectively rendering any form of margin lending or portfolio finance commercially unfeasible and nullifying the effect of 7 USC § 2(c)(2)(D) entirely.[51]

Additionally, the "free use in commerce" requirement raises concerns unique to virtual currencies. Only the most liquid and widely accepted virtual currencies, such as Bitcoin, are significantly, let alone "freely" accepted in commerce. Even with regard to Bitcoin, only the current longest blockchain version of that currency – i.e. that remaining longest chain after any prior forks resulting in the abandonment of shorter blockchains.

---

[48] https://www.cftc.gov/PressRoom/PressReleases/8139-20#:~:text=CEA%20section%202(c)

[49] *Id.*

[50] *Id.*

[51] https://www.federalregister.gov/documents/2013/08/23/2013-20617/retail-commodity-transactions-under-commodity-exchange-act

Such a fork event may render a Bitcoin non-acceptable in commerce even after the "actual delivery" took place under § 2(c)(2)(D).[52]

It is important to note that neither the Final Interpretation, nor any reliable public guidance or statement by the CFTC of which we are aware specifically addresses unmargined short selling of BTC or any virtual currency or the lending of virtual currency to retail counterparties for such purpose. CFTC Chairman Heath Tarbert publicly stated that his expectation that "for a period of 90 days, the CFTC will not initiate any enforcement actions relating to the Final Interpretation that "were not plainly evident from prior CFTC guidance, enforcement actions, and case law" in order to"prevent any potential market disruptions associated with efforts to assimilate this guidance."

Virtual Currencies as Potential Derivatives under the CEA

"Swap Agreements" are defined by the Commodity Futures Modernization Act of 2000 (the "CFMA"), now incorporated into the CEA.Crucially, the CFMA strictly limits the definition of Swap Agreements by restricting the categorization to only those contracts traded by "Eligible Contract Participants" ("ECPs"). The term "commodity" is also broadly defined in the CEA and by CFTC to include almost any standardized, fungible contract of sale for future delivery. Further, the CEA specifically defines financial futures and security index futures as "excluded commodities" subject to regulation under the CEA.

Any commodity-based swap where one counterparty to the agreement does not qualify as an ECP would revert to the default classification of a "commodity" contract under the CEA. Both the contracts and the parties to the agreement would be subject to the full penumbra of regulation and enforcement authority under the CEA, and such contracts would be illegal unless the CFTC granted them the status of "Designated Contract Market" and the contracts were listed on a CFTC- recognized futures exchange. Dealing in Swap Agreements also carry significant registration and reporting requirements under Dodd Frank, including potential registration as a Swap Dealer and/or Swap Execution Facility.

With respect to Virtual Currencies (including NDFs), the swap question is complex. The Division has cautioned a number of times that the complexity of a multi-step contractual process "within one transactional counterparty construct" might render a crypto instrument a Swap Agreement and thus regulable under the CEA and effectively legal only for ECP customers. One specific issue the Division raised in this regard is whether the crypto might represent or have elements of a smart contract, i.e.

[52] *Id.*

where contractual terms independent and/or ancillary to the actual transfer of the virtual currency itself are set, executed and/or enforced by technological protocols. Another issue raised in telephonic guidance is whether the requirement that all components of a transaction (coin loan, coin sale, coin buyback and/or repayment) remain within the same "counterparty construct."

History of CFTC Enforcement

While much relevant case law appears to have centered around the Commission's assertion of anti-fraud jurisdiction, certain cases have extended this to issues of jurisdiction under CEA § 2(c)(2)(D).[53]

Bitfinex Order

Bitfinex Order ruled in a 2015 enforcement action that Bitcoin and other virtual currencies are "commodities" under the CEA, the CFTC first applied the concept of "actual delivery" to virtual currencies the 2016 Bitfinex Order.[54] The Commission filed and simultaneously settled charges against BFXNA, Inc., d/b/a Bitfinex (Bitfinex), in connection with Bitfinex's operation of an online virtual currency trading platform (the BitfinexPlatform). Specifically, the Bitfinex Order found that Bitfinex facilitated the execution of illegal, off-exchange commodity transactions in violation of the CEA by "permitting retail and non-retail users to engage in financed virtual currency transactions on the Bitfinex Platform that did not result in actual delivery of the virtual currency within 28 days, and "failing to register the Bitfinex Platform with the CFTC as a DCM and a futures commission merchant (FCM).

Importantly, the CFTC found that, under each of the three different methods that Bitfinex used to hold the financed virtual currency purchased by its users, Bitfinex had not transferred possession and control of the virtual currency to the customer, and that Bitfinex instead had retained some degree of possession and control over the purchased virtual currency by depositing it into wallets controlled by the company.

CFTC v. McDonnell

In *CTFC v. McDonnell,* the CFTC sued Patrick McDonnell and his company Coin Drop Markets alleging defendants "operated a deceptive and fraudulent virtual currency scheme... for purported virtual currency trading advice" and "for virtual currency

---

[53] *Id.*

[54] https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfbfxnaorder060216.pdf

purchases and trading ... and simply misappropriated [investor] funds."[55] The CFTC sought injunctive relief, monetary penalties, and restitution of funds received in violation of the CEA. The case held that "[v]irtual currencies can be regulated by the CFTC as a commodity." However, it also noted that "CFTC does not have regulatory authority over simple quick cash or spot transactions that do not involve fraud or manipulation. . . this boundary has been recognized by the CFTC. It has not attempted to regulate spot trades unless there is evidence of manipulation or fraud," (citing 7 USC § 2(c)(2)(C)(i)(II)(bb)(AA)). Note carefully that this later conclusion in *McDonnell* appears to apply standards not contained in CEA § 2(c)(2)(D), but instead from § 2(c)(2)(C) – a provision limited by its terms to foreign currency transactions.

United States CFTC c. Money Credit Co.

United States CFTC v Monex Credit Co., a 2019 9th Circuit decision dealt with metals rather than virtual currency.[56] It held, inter alia:

- Actual delivery required at least some meaningful degree of possession or control by the customer but not when, as here, metals were in the broker's chosen depository, never exchanged hands, and subject to the broker's exclusive control, and customers had no substantial, non-contingent interests; [emphasis added]
- The actual delivery exception was an affirmative defense that did not bar the CFTC from relief on three counts;
- The CFTC could sue the seller for fraudulently deceptive activity, regardless of whether it was also manipulative, and the CFTC could bring an enforcement action;
- The CFTC's well-pleaded complaint had to be accepted as true, and the case was remanded for further proceedings;
- Reversed district court's granting of motion to dismiss – 9th Cir. instead held that the CFTC stated a claim because the district court had an incorrect understanding of actual delivery;
- "[S]ales where customers obtain meaningful control or possession of commodities, i.e., when actual delivery occurs, do not mimic futures trading and are therefore exempt from registration and related CEA requirements;"
- "'[A]ctual delivery' unambiguously requires the transfer of some degree of possession or control. Other interpretive tools, including the CFTC's guidance, reinforce this conclusion" [emphasis added].

[55] *CFTC v. McDonnell*, 287 F. Supp. 3d 213, 227 (E.D.N.Y. 2018).
[56] *United States CFTC v Monex Credit Co., 2019 U.S. App. LEXIS 22181, No. 18-55815, *16-19 (9th Cir. July 25, 2019)*

Monex seems significant, as it is the latest in a long line of 9th Circuit cases centered around one of the country's largest providers of leveraged metals contracts to the retail market. It is both noteworthy and highly suggestive that the *Monex* standard is markedly less absolute in its requirement for actual delivery than that stated in the earlier interpretations. The phrase "some (meaningful) degree of possession or control" as seen in *Monex,* seems to leave room for a trustee or custodial account control arrangement, making a security interest in the commodity sufficiently enforceable to sustain a commercially reasonable margin or loan or portfolio finance facility. However, this conclusion is inconsistent with the language and illustrative examples provided in the Final Interpretation.

CTFC v. My Big Coin Pay, Inc.

In *CFTC v. My Big Coin Pay, Inc.,* The Commission filed suit against an operator of a virtual currency scheme, and its officers, alleging fraud in the sale of a commodity, in violation of the CEA and CFTC regulation.[57] The operators and officers moved to dismiss. The court held that it would take judicial notice of the fact that other virtual currency futures were traded on the commodity market and that the complaint sufficiently alleged that "My Big Coin" was a commodity contract.

Further CFTC action included an order filing and settling charges against software protocol *bZeroX* and its founders, Tom Bean and Kyle Kistner. They were charged with offering illegal, off-exchange trading of digital assets, registration violations, and neglecting to adopt a customer ID program required by the Bank Secrecy Act compliance program. The CFTC also filed a civil enforcement action charging the *Ooki DAO*, which is the alleged successor to bZeroX, with violating the same laws as bZeroX allegedly violated, seeking, disgorgement, civil monetary penalties, restitution, trading and registration bans and permanent injunctions against further violations.

SECTION 3: Ripple & Terraform: The Evolving Legal Framework for Digital Assets

After years of apprehension from the blockchain and cryptocurrency industries, the U.S. District Court for the Southern District of New York issued an opinion on the cross-motion for summary judgment claims in *SEC v. Ripple Labs, Inc.*[58] In her opinion, District Judge Analisa Torres ruled Ripple's native token, XRP, "is not in and of itself a 'contract, transaction[,] or scheme[.]'"[59] This finding was a major victory for Ripple Labs and the entire cryptocurrency industry, as the fact that XRP was not by itself a security provided a cognizable path forward for digital assets to avoid securities registration

[57] *CFTC v. My Big Coin Pay, Inc.*, 334 F. Supp. 3d 492 (D.Mass. 2018)
[58] Securities and Exchange Commission v. Ripple Labs Inc., No. 20-cv-10832 (S.D.N.Y. July 13, 2023).
[59] *Id.* at 24.

requirements.[60] The judge rejected the SEC's token-as-security claim, which attempted to label XRP as a security in all instances, and instead looked at each form of transaction Ripple Labs made, and reached individual conclusions on whether the transactions violated securities laws.[61] XRP was distinguished multiple times as the "subject of an investment contract" rather than an investment contract itself.[62] This alone was a win for the industry, as the SEC had previously taken the stance that, without conducting individual analyses, most major cryptocurrencies were unregistered securities.[63] In declaring summary judgment against the token-as-security claim, the judge affirmed the prevailing sentiment among industry lawyers that each digital asset requires an individual assessment under the *Howey* test.[64]

The judge delved into each form of transaction, finding that in three of the four instances at issue, Ripple Labs was not required to register its transactions as a security.[65] Most importantly, Ripple's "programmatic sales" (sales of XRP on an exchange through the use of an algorithm) were not securities.[66] The court made much of the fact buyers and sellers were both conducting "blind" purchases where neither party knew the identity of the other. Thus, these sales could not have been made with a reasonable expectation of profit derived from the value of others because buyers were unaware if they were purchasing XRP from Ripple Labs directly.[67] Contributing to this finding, the Court noted less than 1% of global XRP trading was done through Ripple's programmatic sales. Thus, the vast majority of token holders did not make any purchase knowing that their money would be going to support the XRP community and increase the value of XRP.[68] Driving this point home, the court reasoned that a buyer's "speculative motive" is not evidence alone of an investment contract.[69] Therefore, tokens sold on exchanges, particularly in the secondary market, are unlikely to satisfy the third prong of the *Howey* test and thus would avoid securities registration requirements.

The ruling weakened the SEC's assertion that the cryptocurrency industry was a "wild west;" it is hard to believe that "the vast majority" of cryptocurrencies are

---

[60] Scott Mascianica et al., *SEC v. Ripple: When a Security Is Not a Security*, HOLLAND & KNIGHT, https://www.hklaw.com/en/insights/publications/2023/07/sec-v-ripple-when-a-security-is-not-a-security (July 20, 2023).
[61] *Ripple Labs* No. 20-cv-10832 at 24.
[62] *Id.*
[63] *Exercise Caution with Crypto Asset Securities: Investor Alert*, SEC, https://www.sec.gov/oiea/investor-alerts-and-bulletins/exercise-caution-crypto-asset-securities-investor-alert (Mar. 23, 2023).
[64] *See* Andrew Bull & Tyler Harttraft, Cryptocurrency and Blockchain Law: SEC's Heightened Enforcement Against Digital Assets, 27 RICH. J.L. & TECH., no. 4, (2021).
[65] *Ripple Labs* at 14-15.
[66] *Ripple Decision Makes Waves Finding Some XRP Sales Not Securities*, BAKERHOSTETLER, https://www.bakerlaw.com/alerts/ripple-decision-makes-waves-finding-some-xrp-sales-not-securities (July 20, 2023).
[67] *Ripple Labs* at 23-24.
[68] BAKERHOSTETLER, *supra note 13.*
[69] *Ripple Labs* at 36.

unregistered securities[70] when the first major court case to address the issue concluded that XRP, a major cryptocurrency, was not in and of itself a security.

However, the ruling was not an unconditional success for Ripple Labs, and the SEC can claim some partial victory on its complaint against Ripple and its path forward against the industry should it decide not to alter course through a settlement or new direction. To start, Judge Torres concluded Ripple's institutional sales of XRP constituted a violation of the Securities Act and left open for a jury to decide whether Ripple's control people aided in those unlawful sales.[71]

Judge Torres' conclusion was based on the *Howey* test. The first prong, investment of money, is satisfied because the Institutional Buyers "provide[d] the capital" for XRP.[72] Because the Institutional Buyers invested money in exchange for XRP, Ripple has no standing to argue this prong.[73]

The second prong of *Howey,* "the existence of a 'common enterprise,'" was satisfied because horizontal commonality existed because Institutional Buyers' investments were pooled together and their ability to profit was tied to Ripple.[74] The Court ruled that Ripple's accountants pooled all the XRP-related proceeds together and used it to fund Ripple's operations.[75] Judge Torres moved to the Institutional Buyers' ability to profit was "tied to Ripple's fortunes and the fortunes of other Institutional Buyers because all Institutional Buyers received the same fungible XRP."[76] Because Ripple used these funds to increase the value of XRP, and all Institutional Buyers profited together when XRP rose, horizontal commonality existed.[77] Thus, the second prong was satisfied.

The third and fourth prongs, whether the economic reality surrounding Ripple's Institutional Sales led the Institutional Buyers to have a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others, were satisfied due to the substantial amount of marketing done by Ripple. Beginning in 2013, Ripple began marketing XRP to investors with statements from Ripple leadership indicating that Ripple will "add… the most value to the protocol."[78] Ripple's "overall messaging" to Institutional Buyers was that XRP was speculative, but could be trusted to increase in

[70] Practicing Law Institute. "The SEC Speaks 2022".
[71] *Ripple Labs* No. 20-cv-10832 at 22.
[72] *Id*. at 16.
[73] *Id*.
[74] *Id*. at 17 (citing *Revak v. SEC Realty Corp*., 18 F.3d 81, 87 (2d Cir. 1994)).
[75] *Id*. at 17.
[76] *Id*. at 17-18.
[77] *Id*. (citing *Telegram*, 448 F. Supp. 3d at 369–70).
[78] *Id*. at 20.

value due to Ripple's efforts.[79] Finally, the Court opined on the fact that Institutional Buyers would not agree to lock-up periods if XRP was "used as a currency or for some other consumptive use."[80] In other words, why would investors freeze their funds if they did not expect a profit at the end of the lock-up? The most logical conclusion is investors would not lock-up their assets for a commodity or currency token. Thus, the Court concluded all four prongs of *Howey* were satisfied. Institutional Sales of XRP were in violation of Section 5 of the Securities Act.[81]

The main take-away from these SEC administrative rulings and judicial precedent is: (1) tokens that satisfy the *Howey* test are securities; (2) each token is evaluated on a case-by-case basis, but this theory has been recently pushed back on by the SEC; (3) utility and the lack of an investment does not absolve tokens from a securities designation; and (4) tokens that instill an expectation of profits due to the efforts of the token issue will almost always result in a securities designation.

New York continues to be the venue for a large amount of other regulatory enforcement litigation arising from crypto, including the recent Terraform Labs matter[82] which recently went to trial where a jury held Terraform Labs, and its founder, liable for "defrauding investors in crypto asset securities."[83]

These enforcement actions are often venued in Federal Court, in New York's Southern District of New York ("SDNY"), as well as criminal matters such as the Mango prosecution arising out of allegations of commodities fraud, commodities market manipulation, and wire fraud in connection with the manipulation on the Mango Markets digital asset exchange.[84] This overlap of enforcement and criminal actions in the SDNY is not limited to the DOJ and SEC. For example, recently KuCoin, a digital asset exchange, was charged by the CFTC with multiple violations of the Commodity Exchange Act (CEA) and CFTC regulations in SDNY.[85] The DOJ also has commenced a criminal action against KuCoin, also pending in the SDNY, with failing to register with the appropriate U.S. government entities and failure to maintain an anti-money laundering database.[86] This report delves deeper into the impact of emerging technologies including digital finance and currency on the criminal justice system.

---

[79] *Id*. at 21.
[80] *Id*. at 22.
[81] *Id*.
[82] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-32.pdf
[83] https://www.sec.gov/news/statement/grewal-statement-040424
[84] https://www.justice.gov/usao-sdny/pr/man-convicted-110-million-cryptocurrency-scheme; *See*, https://www.sec.gov/news/press-release/2023-13; US. V. Wahi https://www.justice.gov/media/1233526/dl; *See also,* SEC v. Wahi https://www.sec.gov/files/litigation/complaints/2022/comp-pr2022-127.pdf
[85] https://www.cftc.gov/media/10421/enfkucoincomplaint032624%20/download
[86] https://www.justice.gov/media/1345231/dl

To the extent that any of the actions conflict, the Second Circuit and possibly the Supreme Court, will have the final say. Nonetheless, it is evident that crypto related litigation is highly prevalent in New York, both in Federal and New York State Court.[87]

SECTION 4: Binance and the Regulatory Scrutiny of Digital Assets

More recently, the SEC categorized a token as a security in additional actions brought against Binance and Coinbase. Both complaints provide insight into the SEC's considerations for when a token is a security.

In *Binance*, the SEC alleged Binance offered and sold unregistered securities to US customers through its sale of various digital assets, including Binance's native token—BNB—and other major cryptocurrencies.[88] In its complaint, the SEC alleges Binance engaged in the offer and sale of four native unregistered securities: the native Binance token BNB, the stablecoin BUSD, Binance's savings programs Simple Earn and BNB Vault, and its native staking program. In addition, the SEC alleges Binance offered at least ten unregistered securities on its exchange affiliated with other platforms, including major tokens such as SOL, ADA, and ALGO.[89] After its ICO (initial coin offering) of BNB raised roughly $15 million in two weeks in 2017, Binance launched the Binance.com Platform, where customers may engage in spot-trading and OTC trading services for various cryptocurrencies.[90] BNB has been the native token on the Binance platform since its inception, and its value to purchasers derives from its relationship with Binance itself.

According to the SEC, Binance's own representations make it clear BNB is a security. BNB was "offered and sold as a security because Binance touted an investment in BNB as an investment in Binance's efforts to create a successful crypto asset trading platform centered around BNB."[91] The SEC points to the original Binance whitepaper which alluded to BNB as an "exchange token" which the SEC defines as "a crypto asset associated by its issuer with a crypto asset trading platform that the issuer markets as an investment in the success of the platform itself."[92]

Also noted was Binance's pre-ICO "touting" of the potential returns BNB holders could expect due to platform growth.[93] The Binance whitepaper labeled ICO participants

---

[87] *See*, People of the State of New York v. Vino Global Limited D/B/A Coinex; https://ag.ny.gov/sites/default/files/memorandum_of_law_in_support_of_petition._nyoag_v._vinogloballtd_dba_coinex.pdf
[88] Complaint, SEC v. Binance Holdings Ltd., No. 1:23-cv-01599 (D.D.C. filed June 5, 2023)
[89] *Id.* at 352.
[90] *Binance Coin (BNB) ICO*, Coincodex (accessed July 14, 2023) https://coincodex.com/ico/binance-coin/.
[91] Complaint, SEC v. Binance Holdings Ltd. at 82.
[92] *Id*.
[93] *Id*. at 289.

as investors, described how the Binance leaders' expertise gives the platform strategic advantages for growth, and how the founding members had experience in the securities industry.[94]

Binance's own words were continually used against them. Next, the SEC turned to Binance's assertion it would manipulate the price of BNB by burning half the total supply of BNB over time by purchasing it with the profits of Binance.[95] By increasing demand by forcibly removing supply, the SEC claimed, "Binance gave BNB investors a reasonable expectation of profits because lower demand tends to increase price, similar to how a stock issuer uses profits to provide dividends to investors or to execute stock buybacks to increase the ownership stake of remaining shareholders."[96] Binance, in the view of the SEC, had tied BNB's success to the Binance platform's success.[97]

Finally, the SEC used former Binance CEO Changpeng Zhao's public claims that through Binance's efforts, BNB's value will continue to rise. In multiple interviews, Zhao told investors, "Binance's efforts to make the Binance.com Platform more profitable will increase BNB's value."[98] The SEC identified dozens of occasions where Zhao or Binance leadership described the work the Binance platform was doing to increase the value of the BNB token.

In general, the SEC had for years been quite clear on one point: each token is evaluated on a case-by-case basis. However, this theory does not line up with the SEC's recent approach against Binance and Coinbase.[99] In *Binance*, the SEC did not limit its hunt to just BNB. As described earlier, the SEC alleges Binance offered at least ten unregistered securities on its exchange that were affiliated with other platforms.[100]

This strategy offers the SEC some advantages. It hypothetically can lose on all its claims against the native BNB, yet still prevail both on the case and its larger movement to regulate the industry. A more concerning issue is the SEC has either forgotten or abandoned its original assertion that the securities designation is a fact-specific test. Both former Chairwomen Mary Jo White, went on to represent Ripple Labs, and the DAO report explained the designation of digital assets as securities required an individual application

[94] *Id*. at 290-91.
[95] *Id*. at 295.
[96] *Id*.
[97] *Id*.
[98] *Id*. at 302.
[99] On June 6th, just a day after filing its complaint against Binance, the SEC sued the largest cryptocurrency exchange in the United States, Coinbase Inc. Coinbase is a publicly traded Foundation operating a cryptocurrency exchange where American customers can purchase and trade many major cryptocurrencies like bitcoin and ether on a secondary market. Much like its lawsuit against Binance, the SEC accuses Coinbase of offering and selling unregistered securities and failing to register its business as an exchange, broker-dealer, and clearing agency. However, it does not allege that Coinbase offers any native unregistered security token like BNB.
[100] *Id*. at 350.

of the *Howey* test for each asset, and decried the notion that digital assets as a concept constituted securities by definition.[101] Instead, the SEC complaint against Binance abandons the individualized framework, resorting to sweeping statements classifying third-party digital assets as securities without more than a few paragraphs of explanation and certainly no independent complaints. Along with practical complications, the SEC has created only more confusion by contradicting its previous stance on the nature and process to evaluate digital assets as securities.

SECTION 5: SEC Approves Spot Bitcoin ETFs

In January 2024, the SEC approved the trading of spot bitcoin exchange-traded funds (ETFs), marking the first occasion such investments have received approval from the regulatory body.[102] The approvals were granted to a range of companies including BlackRock, Fidelity, Grayscale, Bitwise, VanEck, Valkyrie, Invesco, WisdomTree, Franklin Templeton, Hashdex, Ark Invest, and 21Shares. SEC Chairman Gary Gensler clarified, "While we approved the listing and trading of certain spot bitcoin ETP shares today, we did not approve or endorse bitcoin."[103] He went on to state "As I've said in the past, and without prejudging any one crypto asset, the vast majority of crypto assets are investment contracts and subject to the federal securities laws."[104] Gensler made clear his position is that "bitcoin is primarily a speculative, volatile asset that's also used for illicit activity including ransomware, money laundering, sanction evasion, and terrorist financing."[105] These issues are addressed infra in Article 4 of this report.

The journey toward the approval of spot Bitcoin ETFs in the United States has been complex and lengthy. It began in 2013 with a submission from the Winklevoss Bitcoin Trust, which was ultimately declined by the SEC.[106] The SEC consistently rejected numerous applications for spot-based bitcoin ETFs, citing the unregulated nature of bitcoin and the consequent investor risks.

The tide turned when crypto asset manager Grayscale took legal action against the SEC to demand more transparency and a shift in stance.[107] This lawsuit led to a

---

[101] *See* Letter from Mary Jo White, *supra* note 8; DAO Report, *supra* note 5.
[102] U.S. Securities and Exchange Commission, Release No. 34-99306 (Jan. 10, 2024) https://www.sec.gov/files/rules/sro/nysearca/2024/34-99306.pdf.
[103] Gary Gensler, "Statement on the Approval of Spot Bitcoin Exchange-Traded Products," (Jan 10, 2024), https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023.
[104] *Id.*
[105] *Id.*
[106] Nathan Reiff, "SEC Rejects Winklevoss Bitcoin ETF Plans," Investopedia, (Jul. 30, 2018), https://www.investopedia.com/news/sec-rejects-winklevoss-bitcoin-etf-plans/.
[107] Grayscale Invs., LLC v. Sec. & Exch. Comm'n, 82 F.4th 1239 (D.C. Cir. 2023) https://www.cadc.uscourts.gov/internet/opinions.nsf/32C91E3A96E9442285258A1A004FD576/$file/22-1142-2014527.pdf

significant development: the U.S. Court of Appeals for the District of Columbia determined that the SEC did not properly justify its decision to reject Grayscale's proposed exchange-trained product (ETP), finding that the SEC's actions were "arbitrary and capricious" in disapproving the proposed Bitcoin ETP.[108] As a result, the court overturned the Grayscale Order and remanded it back to the SEC. Following this, the SEC decided to authorize the trading of spot Bitcoin ETFs as the most logical step forward.[109] This decision came after the appellate court's finding, which challenged the SEC's prior stance and paved the way for the regulatory approval of these financial products.[110]

SECTION 6: Analysis of the Proposed Bill Lummis-Gillibrand Responsible Financial Innovation Act

The Lummis-Gillibrand Responsible Financial Innovation Act represents a significant stride towards the integration of digital assets within the framework of U.S. financial regulations, marking a pivotal moment in the evolution of the Web3 and cryptocurrency landscape.[111] Crafted by Senators Cynthia Lummis and Kirsten Gillibrand, this bipartisan bill seeks to establish a comprehensive regulatory environment for digital assets, addressing crucial aspects of the cryptocurrency ecosystem such as consumer protection, regulatory clarity, and innovation encouragement.[112]

Historical Context and Development:

The emergence of the Act can be traced back to the growing recognition of digital assets and cryptocurrencies as formidable forces in the global financial system. Over the years, the rapid expansion and the increasingly mainstream adoption of these technologies underscored the need for clear regulatory frameworks to safeguard investors, support innovation, and ensure market integrity. In response to these challenges, the Lummis-Gillibrand Act was proposed as a means to bridge the gap between traditional financial regulatory structures and the novel dynamics introduced by digital assets.

---

[108] Dechert LLP, "D.C. Circuit Finds SEC Acted "Arbitrarily and Capriciously" in Disapproving Proposed Bitcoin ETP," (Sep. 13, 2023) https://www.dechert.com/knowledge/onpoint/2023/9/d-c--circuit-finds-sec-to-have-acted--arbitrarily-and-capricious.html.

[109] Gensler, *supra* note 74; Shenna Peter, "Thailand's SEC Greenlights Investment From Institutional and Wealthy Individuals in Crypto ETFs," (Mar. 12, 2024) https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023#.ZaSR6EEHGFM.mailto; https://www-coindesk-com.cdn.ampproject.org/c/s/www.coindesk.com/policy/2024/03/12/thailands-sec-greenlights-investment-from-institutional-and-wealthy-individuals-in-crypto-etfs/amp/.

[110] U.S. Securities and Exchange Commission, "SEC Charges 17 Individuals in $300 Million Crypto Asset Ponzi Scheme Targeting the Latino Community," (Mar. 14, 2024) https://www.sec.gov/news/press-release/2024-35.

[111] *See* S. 4356, 117th Cong. (2022).

[112] *See id.*

Key Provisions and Goals:

The Act is designed to bring clarity to the regulatory roles of the SEC and the CFTC concerning digital assets.[113] By delineating the oversight responsibilities between these two regulatory bodies, the Act aims to reduce ambiguity and create a more predictable legal environment for entities operating within the crypto space.

One of the core objectives of the Lummis-Gillibrand Act is to foster an atmosphere conducive to innovation while ensuring robust consumer protections are in place. This includes establishing clear rules around the issuance and trading of digital assets, implementing safeguards against market manipulation, and promoting transparency within the cryptocurrency industry.

Impact and Future Implications:

Should it be enacted, the Lummis-Gillibrand Responsible Financial Innovation Act could serve as a catalyst for significant change within the U.S. and potentially the global digital asset markets. By providing a clear regulatory framework, the Act not only aims to protect consumers and investors but also to solidify the United States' position as a leading hub for cryptocurrency and blockchain innovation. Moreover, by addressing key regulatory uncertainties, this Act could pave the way for more businesses and investors to participate confidently in the digital asset space. As digital assets continue to evolve and reshape the contours of the global financial landscape, legislative efforts like this play a crucial role in shaping the future of finance, ensuring that innovation thrives in a secure, transparent, and regulated environment.

A. Regulatory Clarity and Jurisdiction

Central to the proposed Act is the precise delineation of regulatory duties between the SEC and the CFTC, with the latter being accorded enhanced jurisdiction over cryptocurrencies.[114] This pivotal restructuring is anticipated to bring a new era of regulatory clarity for Web3 businesses, necessitating a keen adherence to CFTC regulations for crypto assets not classified as securities.

One of the main focuses of the proposed Act is to ensure consumer protection and a market integrity authority. This would be accomplished by the inauguration of a dedicated authority to supervise crypto asset intermediaries signals a shift towards more stringent regulatory oversight. This development implies that Web3 businesses, especially those functioning as intermediaries, will be navigating through an augmented

[113] *See id.*
[114] *See id.*

landscape of regulatory demands, potentially influencing their operational methodologies and compliance frameworks.

B. Reconfiguring Business Models

Crypto Asset Intermediaries and Payment Stablecoin Issuers: By imposing rigorous requirements on intermediaries, including mandatory proof of reserve and explicit transaction disclosures, the Act aims to instill a greater degree of transparency and security in consumer assets.[115] This necessitates Web3 entities to potentially recalibrate their business practices to align with these heightened standards.

The Act delineates issuing rights for the payment of stablecoins to depository institutions or their subsidiaries, a move that could dramatically reshape the stablecoin segment of the Web3 market.[116] This regulatory stance may catalyze a reconfiguration of stablecoin issuance, centralizing it within the realm of traditional financial institutions and thereby altering the competitive dynamics within the Web3 ecosystem.

C. Tackling Illicit Finance

Incorporating measures to combat illicit finance, the Act enhances oversight mechanisms, such as the regulation of cryptocurrency ATMs and the formation of the Independent Financial Technology Working Group.[117] Web3 businesses are thus prompted to adopt robust anti-money laundering (AML) and know your customer (KYC) protocols, aligning with the Act's objectives to curb illicit financial activities.

D. Tax Code Modifications

The Act's proposed amendments to the tax treatment of digital asset transactions, including the exclusion of small transactions from taxable events and the application of wash sale rules, present a nuanced impact on Web3 entities and their clientele.[118] These changes could stimulate the everyday use of cryptocurrencies while simultaneously influencing trading behaviors.

The Lummis-Gillibrand Responsible Financial Innovation Act stands as a transformative piece of legislation, poised to redefine the regulatory framework surrounding digital assets and cryptocurrencies. By offering clarity, enhancing consumer protection, and nurturing innovation, the Act sets a foundation for the sustainable growth of the Web3 industry. As these regulations come into effect, Web3 businesses will

[115] *See id.*
[116] *See id.*
[117] *See id.*
[118] *See id.*

encounter both challenges and opportunities, necessitating strategic adaptation to thrive in this evolved digital finance landscape.

Anticipating the Impact of the Lummis-Gillibrand Act

The Lummis-Gillibrand Responsible Financial Innovation Act is poised to significantly shape the future landscape of digital assets and cryptocurrencies in the United States. Through predictive analysis, drawing on expert opinions and the examination of similar legislative frameworks in other jurisdictions, we can anticipate the potential effects of this act on the Web3 ecosystem. If this Act is adopted, it will provide regulatory clarity and market stability, consumer protection and confidence, innovation and sector growth, stablecoin regulation, global regulatory leadership and DeFi and niche sectors.

Much like the positive outcomes observed with Singapore's regulatory framework for digital assets, the Act's clear guidelines could similarly stabilize the U.S. market, attracting more institutional investors and enhancing overall market stability.[119] Sources like the Monetary Authority of Singapore's reports on digital asset regulation could offer comparative insights.[120]

By establishing robust consumer protection mechanisms, the Act aligns with global trends towards safeguarding retail investors in the digital asset space.[121] The European Union's Markets in Crypto-Assets (MiCA) framework serves as a parallel, emphasizing investor protection and operational transparency.[122]

The inclusion of a regulatory sandbox in the Act echoes successful models like the UK's Financial Conduct Authority sandbox, which has been instrumental in fostering fintech innovation. This approach is likely to catalyze new developments in areas such as DeFi and blockchain technology.

The Act's approach to stablecoin issuers may encourage a more consolidated and regulated stablecoin market.[123] Reflecting on the G7's guidelines on digital payments, the Act's emphasis on stability and compliance could lead to a more reliable stablecoin ecosystem.

---

[119] *See id.*
[120] https://www.mas.gov.sg/news/media-releases/2023/mas-proposes-framework-for-digital-asset-networks
[121] *See* S. 4356, 117th Cong. (2022).
[122] https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica
[123] *See* S. 4356, 117th Cong. (2022).

The Act could establish the U.S. as a frontrunner in digital asset regulation, setting standards for global regulatory harmonization. The U.S.'s leadership might inspire collaborative efforts towards international regulatory standards, as discussed in forums like the G20 and international fintech symposiums.

The Act's focus on emerging sectors like DeFi could formalize regulatory paths for these innovations, encouraging growth within a structured legal framework. Observations from JPMorgan Chase's and other institutional entities' interest in DeFi could offer comparative analysis on potential outcomes.

In summary, the Lummis-Gillibrand Act could mark a significant evolution in the U.S. digital assets market, balancing innovation with investor protection. Its effects could ripple globally, influencing regulatory approaches and fostering a more stable, innovative, and inclusive digital asset ecosystem.

SECTION 7: New York Department of Financial Services Approach

Over the last 5 years, The NYDFS has entered into consent orders, settled regulatory compliance cases, and filed complaints against Gemini[124] (related to the Gemini Earn program which cost investors more than $3 billion dollars in losses), Genesis Global Trading[125] (for currency and cybersecurity violations), KuCoin[126] (for failure to register within the state as a securities or commodity broker-dealer), CoinEx[127] (for failure to register within the state as a securities or commodity broker-dealer), Coin Café[128] (for usurious fees for storage and access to their wallet storage service), BitPay[129] (for violations of state cybersecurity regulations under NYCRR §§ 500.1 to 500.23), and Binance.US[130] (objecting to an asset purchase agreement from the bankrupt Voyager Digital) among various others.

The NYSDFS in November 2023 issued new guidance on listing and delisting policies for virtual currency.[131] This policy focuses on market stability and retail investor

[124] *In re: Genesis Global Holdco, LLC, et al.*, Case No: 23-10063 (SHL), retrieved from: https://rb.gy/tey85u
[125] *Id.*
[126] *New York v. MEK Global Limited and PHOENIXFIN PTR Ltd., d/b/a KuCoin*, Index No. 450703/2023, retrieved from: https://ag.ny.gov/sites/default/files/settlements-agreements/kucoin-stipulation-and-consent.pdf
[127] *New York v. Vino Global Ltd. d/b/a CoinEx,* Index No. 450502/2023, retrieved from: https://ag.ny.gov/sites/default/files/settlements-agreements/coinex-agreement.pdf
[128] *In re: Investigation by Letitia James A.G. of New York of Coin Café, Inc., d/b/a "coincafe" and "coincafe.com"*, Assurance No 23-027, retrieved from: https://ag.ny.gov/sites/default/files/settlements-agreements/Coin%20Cafe%20AOD.pdf
[129] *In the Matter of BITPAY, INC.*, consent order, retrieved from: https://www.dfs.ny.gov/system/files/documents/2023/03/ea20230316_bitpay.pdf
[130] *In re: Voyager Digital Holdings, Inc., et al.*, Case No. 22-10943-MEW, retrieved from: https://cases.stretto.com/public/x193/11753/PLEADINGS/1175302222380000000157.pdf
[131] Adrienne A. Harris, Superintendent of Financial Services, *Industry Letter*, New York Department of Financial Services (Nov. 15, 2023), retrieved from: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20231115_listing_virtual_currencies

protections, through a 'slow and steady' listing and delisting process. This process is akin to skipping a stone rather than just chucking it into the water, to minimize the market level ripples. As well, the NYSDFS Superintendent Adrienne A. Harries stated, "[T]his guidance continues the Department's commitment to an innovative and data-driven approach to virtual currency oversight, keeping pace with industry developments, . . ."[132]

The above notwithstanding, the New York State "Bitlicense"[133] program has been widely criticized by the financial services industry. This has resulted in an exodus of blockchain and virtual currency businesses from the state.[134] Because the regulatory landscape on a state level is so varied, a large number of companies that were previously in New York have moved to either Delaware (obviously known for pro-business laws) and Wyoming[135] (which has attempted to make itself the "crypto friendly" state through substantive legislation).[136] Due to this, the NYSDFS has been pressured to change its BitLicense system[137], and there is currently a proposal pending in the New York State Assembly to replace the BitLicense program with a more innovation-friendly and business-friendly alternative.[138]

SECTION 8: VARA's Approach to Crypto Regulation

The Dubai Virtual Asset Regulatory Authority (VARA) was established to provide a comprehensive regulatory framework for Virtual Asset Service Providers (VASPs) in Dubai. This initiative came in response to the growing prominence of virtual assets (such as cryptocurrencies) and the need for robust governance structures to ensure their safe and effective use within the financial ecosystem.

The formation of VARA marks a significant step by Dubai to position itself as a leading global hub for the virtual assets sector. Recognizing the transformative potential of blockchain and other related technologies, Dubai aimed to create a conducive

---

[132] *Id.*
[133] 23 N.Y.C.R.R. 200.3(a)
[134] David Adler, *The BitLicense: Regulatory Overreach or Prudent Response?*, Fordham Journal of Corporate & Financial Law (Ma. 26, 2018), retrieved from: https://news.law.fordham.edu/jcfl/2018/03/26/the-bitlicense-regulatory-overreach-or-prudent-response/; Sandali Handagama & Jaspreet Kalra, *BitLicense at 5: A Timeline of New York's Landmark Cryptocurrency Regulation*, Coindesk (Jun. 24, 2020), retrieved from: https://www.coindesk.com/policy/2020/06/24/bitlicense-at-5-a-timeline-of-new-yorks-landmark-cryptocurrency-regulation/; Guy C. Dempsey, Jr. & Gary De Waal, *New York BitLicense Regulations Virtually Certain to Significantly Impact Transactions in Virtual Currencies*, Nat. L. Rev. (Apr. 25, 2024), retrieved from: https://natlawreview.com/article/new-york-bitlicense-regulations-virtually-certain-to-significantly-impact-transactio
[135] Wyo. Stat. Ann. §§ 40-22-101 to 40-22-129
[136] Wyo. Stat. Ann. §§ 40-22-102(a)(xxii) and 40-22-104(a)(vi)
[137] Carlton Fields, *State Regulations on Virtual Currency and Blockchain Technologies (Updated March 2021)*, (Mar. 15, 2021), retrieved from: https://www.carltonfields.com/insights/publications/2021/state-regulations-virtual-currency-blockchain-tech
[138] New York State Attorney General, *Attorney General James Proposes Nation-Leading Regulations on Cryptocurrency Industry* (May 5, 2023), retrieved from: https://ag.ny.gov/press-release/2023/attorney-general-james-proposes-nation-leading-regulations-cryptocurrency

environment for innovation while safeguarding market integrity and protecting investors.[139]

VARA's mandate encompasses a wide range of regulatory and supervisory functions, from licensing VASPs to monitoring their operations, to ensure compliance with established legal and regulatory standards.[140] This involves setting clear guidelines on the operational, technical, and security practices that VASPs must adhere to, promoting transparency and trust in the virtual assets market.

VARA Requirements

VARA mandates that VASPs adhere to stringent company structure and governance standards, as detailed in the Company Rulebook. These standards ensure clear and effective oversight fostering a transparent, secure, and orderly virtual asset market**.**

VARA requires strict adherence to the Company Rulebook, which outlines specific requirements for VASPs concerning company structure, governance, and operational conduct. This includes adherence to additional rule books which address compliance and risk management, technology and information, and market conduct, ensuring a comprehensive regulatory approach.

The ownership and governance rules require that VASPs must have a clear and transparent structure. These companies must maintain a company structure conducive to effective VARA oversight, ensuring the sound and effective operation of the VASP, including its virtual asset activities.[141] VASPs are required to establish and maintain a legal entity within Dubai, adhering to one of the legal forms approved by a commercial licensing authority in the Emirate. Additionally, they must have a clear chain of ownership, delegated authority, and associated voting powers must be maintained, allowing VARA to easily identify any controlling entities and ultimate beneficial owners (UBOs).[142] VASPs employing complex structures, including trusts, nominee arrangements, or decentralized autonomous organizations (DAOs), must provide detailed information to VARA. This includes the reasons for such structures, the relationship between the VASP and relevant DAOs, and any potential compliance impacts.[143] Lastly, with regard to governance and ownership any material changes to the company structure or adoption of decentralized governance relating to VA activities require VARA's prior written approval.[144] VASPs must submit detailed information on

[139] *See* Virtual Assets Regulatory Authority, https://www.vara.ae/en/, (last visited Apr. 5, 2024).
[140] *See* Virtual Assets Regulatory Authority, https://rulebooks.vara.ae/rulebook/rulebooks, (last visited Apr. 5, 2024).
[141] *See* Virtual Assets Regulatory Authority, *supra* note 93.
[142] *See id.*
[143] *See id.*
[144] *See id.*

new controlling entities, group entities, and UBOs as requested by VARA, along with compliance with any additional conditions or restrictions imposed by VARA.[145]

The Rulebook specifies the structure and responsibilities of the company board and senior management, emphasizing the need for individuals who meet the "Fit and Proper Persons" criteria.[146] It outlines procedures for their selection, induction, and ongoing assessment to ensure effective governance and compliance.[147]

The VASPs must meet specific paid-up capital requirements, maintain net liquid assets, and secure adequate insurance to mitigate operational and financial risks.[148] These requirements are calibrated based on the scope of VA activities conducted by the VASP.[149]

Comprehensive policies and procedures for risk management must be established, including internal controls, segregation of duties, and conflict of interest management.[150] This framework is designed to safeguard against operational, financial, and compliance risks.[151]

By establishing these rules, VARA ensures that measures are put in place to protect client assets, including requirements for maintaining reserve assets and ensuring transparency in transactions with related parties.[152] Guidelines for outsourcing arrangements are enforced to ensure that outsourced services do not compromise the integrity or security of VA operations.[153]

Finally, the Rulebook provides for orderly wind-down procedures to protect stakeholders in the event of a VASP’s insolvency or voluntary discontinuation of business, underlining the importance of maintaining a stable and secure virtual asset market.[154]

SECTION 9: Navigating the Future of Digital Asset Regulation

The legal proceedings of *SEC v. Ripple Labs, Inc*. and the SEC's actions against Binance and Coinbase have underscored the complexities and challenges of regulating

[145] *See id.*
[146] *See id.*
[147] *See id.*
[148] *See id.*
[149] *See id.*
[150] *See id.*
[151] *See id.*
[152] *See id.*
[153] *See id.*
[154] *See id.*

digital assets in the evolving landscape of Web3 and decentralized technologies. These cases highlight the need for individual assessments under the *Howey* test to determine the status of digital assets and emphasize the importance of nuanced legal evaluations within the digital asset ecosystem. As the digital asset industry continues to grow and diversify, it becomes increasingly clear that a one-size-fits-all approach to regulation is inadequate.

The *Ripple* case, in particular, is a pivotal reference point for understanding the industry's legal and regulatory challenges. It demonstrates the necessity for clear and comprehensive legal frameworks that can adapt to the unique characteristics of digital assets. The case also highlights the importance of collaboration between regulators, industry stakeholders, and legal professionals to ensure that regulations are effective, fair, and conducive to innovation.

As we move forward, the United States and New York must establish a more robust and effective legal and regulatory framework for digital assets. This report recommends enacting clear federal legislation on digital assets, improving regulatory oversight by the SEC, establishing a regulatory sandbox for digital assets, and fostering innovation and collaboration. These recommendations aim to promote innovation while ensuring market integrity and investor protection.

By addressing digital assets' challenges and opportunities, the United States and New York can position themselves as leaders in the global digital economy. The legal and regulatory framework must evolve to keep pace with technological advancements, ensuring that the potential of digital assets is fully realized while mitigating the risks associated with this new asset class.

Article 2: Navigating the New Web3 Business Frontier through the Sandbox Approach

SECTION 1: From Web1 to Web3: A Digital Evolution

The digital world has undergone a remarkable transformation, starting with Web1's static and solitary pages, advancing through Web2's dynamic social platforms and user-generated content, and arriving at the precipice of Web3. This new phase challenges the centralized control seen in Web2 by championing a decentralized, blockchain-driven architecture. Web3 isn't merely a step forward in technology—it's a redefinition of online interaction, prioritizing user control, data privacy, and direct transactions devoid of intermediaries.

Central to the Web3 revolution is blockchain technology—a decentralized public ledger system that ensures transparency, security, and integrity across a distributed network. Far surpassing its initial association with cryptocurrencies, blockchain's influence extends across industries, from finance to healthcare, by facilitating secure and efficient digital transactions. The intricate nature of blockchain technology beckons legal experts to grapple with its regulatory, intellectual property, and privacy implications, underscoring the need for a comprehensive legal understanding as this technology permeates various sectors.

SECTION 2: The Impact of Decentralization on Business

The emergence of Web3 opens vast avenues for business innovation and growth. Leveraging decentralized technologies, businesses can revolutionize operational efficiency, data accuracy, and consumer engagement. This paradigm shift invites companies to rethink strategies, from product development to customer interaction, in a landscape where transparency and security become distinguishing features.

The leap into the Web3 domain necessitates navigating a fluid regulatory landscape. Initiatives like the Dubai Virtual Asset Regulatory Authority (VARA)[155] and legislative efforts such as the Lummis-Gillibrand Act exemplify the attempts to frame regulation that fosters innovation while ensuring consumer and market protection.[156] These frameworks highlight the importance of aligning business practices with legal standards to harness Web3's potential responsibly.

[155] *See id.*
[156] Kristin Gillibrand, Press Release, July 12, 2023.

SECTION 3: Steering Through Legal Complexities

As the Web3 ecosystem expands, businesses face the critical task of understanding the legalities that govern digital assets, smart contracts, and decentralized applications. The advent of regulatory sandboxes exemplifies a forward-thinking approach, offering businesses a controlled setting to experiment with Web3 technologies. This environment not only aids in demystifying legal uncertainties but also sets the stage for informed legislative development.

The transition towards Web3 signifies a pivotal moment in digital history, promising to reshape not just how businesses operate but also how they interact with consumers and navigate legal frameworks. The ongoing evolution of regulations and the proactive role of businesses and legal professionals in engaging with these changes are crucial for ensuring that the leap into Web3 results in a future marked by innovation, compliance, and enhanced consumer trust.

SECTION 4: Key Issues Stemming from Regulatory Uncertainty in the Web3 Space

As the Web3 ecosystem continues to expand, businesses operating within this domain face a significant challenge: regulatory uncertainty. This challenge stems from the rapid evolution of technology outpacing the development of comprehensive regulatory frameworks by governments worldwide. The lack of clarity and consistency in government regulations concerning cryptocurrencies and virtual assets presents a multifaceted problem for Web3 businesses, impacting their operational, legal, and strategic planning aspects.

The key issues stemming from this regulatory uncertainty are compliance risks, investor confidence, innovation is stifled and market fragmentation. Without clear regulations, Web3 businesses navigate a precarious landscape where the risk of non-compliance with future regulatory mandates is high. This uncertainty can lead to significant legal and financial repercussions, hindering the ability of these businesses to plan and execute their strategies effectively.

The absence of established regulatory guidelines can erode investor confidence in the Web3 space. Potential investors may be hesitant to engage with businesses in an environment perceived as legally ambiguous, limiting access to capital for startups and established entities alike.

Regulatory uncertainty can stifle innovation. Businesses may be reluctant to explore new opportunities or deploy cutting-edge technologies due to concerns about

future legal constraints, thus potentially slowing the growth and maturation of the Web3 ecosystem.

The lack of a unified regulatory approach leads to a fragmented market, where businesses must navigate a patchwork of regional and national regulations. This fragmentation complicates operations for businesses with a global presence, increasing operational complexities and costs.

To address these challenges, it is imperative for regulatory bodies to engage with the Web3 community to develop clear, comprehensive, and adaptive regulatory frameworks. Such collaborative efforts should aim to protect consumers and ensure market integrity while also fostering innovation and growth within the Web3 ecosystem. Establishing a regulatory environment that balances these considerations is crucial for the long-term success and sustainability of businesses operating in the Web3 space.

SECTION 5: The Economic and Innovation Leap: Dubai's Crypto and VARA Success Stories

Dubai's strategic embrace of the digital economy, spearheaded by the Virtual Assets Regulatory Authority (VARA), has established the city and the United Arab Emirates as premier destinations for the burgeoning global crypto and virtual asset industry. This integration has not only positioned Dubai as a hub for innovation and regulatory excellence, but also spurred significant economic growth and attracted leading crypto companies worldwide.

Establishing a Regulatory Framework for Growth and Innovation

VARA's inception under the Virtual Assets Law, tied to the Dubai World Trade Centre Authority, marks a pivotal step in Dubai's commitment to becoming a leading global destination for virtual assets. The authority's creation of a favorable regulatory environment has been key to providing safety, robustness, and attractiveness for virtual asset service providers and investors. This clarity and security in regulation have been fundamental in fostering a thriving ecosystem for virtual assets, drawing in investments and encouraging companies to establish their operations in Dubai.

Success Stories Under VARA's Wing

One of the shining examples of VARA's positive impact is Aquanow, a Canada-based crypto infrastructure provider. Granted a VASP license by VARA, Aquanow has expanded its services to include broker-dealer, lending and borrowing, and management and investment services, thereby positioning Dubai as an integral player

in its international strategy. This move underscores Dubai's appeal as a supportive environment for crypto companies seeking clear regulatory landscapes.

Further attesting to Dubai's status as a global crypto hub are companies like Binance, OKX, and Crypto.com, which have secured licenses from VARA, enhancing their operational and regulatory standing. These developments highlight the influx of leading firms to Dubai, attracted by its regulatory framework designed with an eye toward global best practices and local economic development.

Economic Boosts from Crypto and VARA

Dubai's proactive approach, led by VARA, has not only enhanced its regulatory framework but also significantly contributed to the city's economy. The establishment of VARA and the subsequent attraction of crypto businesses have played a crucial role in promoting innovation, investment, and collaboration within the international regulatory landscape. This environment has fostered growth in niche Web3 sectors such as DeFi and the metaverse, aligning with Dubai's broader economic strategies and contributing to the creation of a vibrant virtual asset ecosystem.

Dubai's strategic initiatives have laid the groundwork for a future where digital technologies foster greater transparency, security, and efficiency across all business facets. By blending regulatory foresight with an open invitation to global crypto enterprises, Dubai has not only solidified its position as a leading destination for crypto and virtual asset companies but has also stimulated economic growth, showcasing the city's role as a cornerstone of the digital finance world.

SECTION 6: Future Outlook

A. Navigating Regulatory Challenges

As the digital asset landscape continues to evolve, the New York State Bar Association (NYSBA) and stakeholders within the regulatory and legislative spheres, such as Senator Gillibrand's office, are positioned to play pivotal roles in shaping the future regulatory environment. Emphasizing compliance, fostering innovation, and preparing for future trends are crucial steps in navigating the regulatory challenges ahead.

Regulatory sandboxes, innovative frameworks allowing businesses to test novel products and services in a controlled environment under regulatory supervision, have emerged as a cornerstone in the evolution of digital finance. These testing grounds enable stakeholders to explore the potentials and implications of new technologies like blockchain and cryptocurrencies without the full burden of regulatory compliance that

would apply under normal circumstances. This concept, drawing from the iterative testing approach commonly found in the tech industry, provides valuable insights for both regulators and innovators, ensuring that regulatory frameworks can adapt to technological advances while safeguarding consumer interests and maintaining financial stability.

Benefits of Digital Asset Regulation and Sandbox Initiatives

1. **Innovation and Economic Growth**: Regulatory sandboxes and clear digital asset regulations can foster innovation by providing a safe space for testing new products and services. This, in turn, can contribute to economic growth. The U.S. Department of the Treasury and the Office of the Comptroller of the Currency (OCC) have discussed the importance of supporting financial innovation while maintaining safety and soundness in the banking system.
2. **Attracting Investment**: A clear regulatory framework can make a country more attractive to investors interested in digital assets. By providing legal certainty and protections, investments in blockchain and fintech startups are likely to increase.
3. **Consumer Protection**: Regulatory frameworks designed with consumer protection in mind can help safeguard against fraud and misuse of digital assets. The Consumer Financial Protection Bureau (CFPB) often emphasizes the importance of consumer protection in financial innovation.
4. **International Standards and Cooperation**: Efforts towards regulatory harmonization can align with international standards, facilitating global cooperation and reducing cross-border friction. Documents and guidelines from international bodies like the Financial Action Task Force (FATF) often highlight the importance of global cooperation in regulating virtual assets.

Challenges of Digital Asset Regulation and Sandbox Initiatives

1. **Navigating Jurisdictional Complexity**: In the U.S., the dual state and federal regulatory systems add layers of complexity to regulating digital assets. Achieving harmonization between various state laws and federal guidelines poses a significant challenge.
2. **Keeping Pace with Technological Advancements**: Digital asset technologies evolve rapidly, making it difficult for regulations to keep pace. The challenge lies in creating flexible, adaptive regulatory frameworks that can accommodate future technological developments without stifling innovation.
3. **International Regulatory Divergence**: While striving for international cooperation, divergences in regulatory approaches between countries can create challenges for businesses operating globally. Ensuring compliance across different jurisdictions requires significant resources and legal expertise.

4. **Resource Allocation**: Developing and maintaining regulatory sandboxes and comprehensive digital asset regulations require significant resources. Government agencies must allocate sufficient funds and manpower to oversee these initiatives effectively.

In light of the evolving digital asset landscape and the critical role of regulatory frameworks in fostering innovation while ensuring consumer protection and market integrity, the New York State Bar Association (NYSBA) emerges as an instrumental player. Given its positioning within the heart of the financial world in New York, and housing some of the most experienced attorneys in the country, the NYSBA is uniquely equipped to lead initiatives that address the complexities of digital asset regulation. The establishment and refinement of regulatory sandboxes represent a forward-thinking approach to navigate the intricacies of this dynamic sector. These innovative frameworks offer a balanced avenue for testing new technologies under regulatory oversight, providing invaluable insights for both regulators and innovators.

As we stand at the cusp of a new era in financial innovation, it is recommended that the NYSBA take a proactive stance in advocating for the federal government to implement and apply regulatory sandboxes more broadly. Such advocacy could catalyze the adoption of adaptable, informed regulatory practices that are essential for the continued growth and development of the digital asset sector. By leveraging its expertise and influence, the NYSBA can champion the cause of regulatory sandboxes, thereby ensuring that the United States remains at the forefront of financial innovation, consumer protection, and market stability. This leadership role could not only facilitate the creation of a conducive environment for digital assets but also underscore the importance of legal and regulatory preparedness in harnessing the transformative potential of these emerging technologies.

Article 3: U.S. Federal Income Tax Considerations for Digital Assets

While a comprehensive discussion of the U.S. federal income tax treatment of digital assets is outside the scope of this report, this section describes two potential "low hanging fruits" for improving current U.S. tax policy.

SECTION 1: Define taxable exchange

We recommend prioritizing guidance on how to determine whether a digital asset transaction is a taxable exchange. In the absence of any such guidance, Congress might consider providing taxpayers with the option to achieve greater certainty on reporting their digital asset gains and losses by expanding the applicability of the mark-to-market election under section 475(e)-(f) to "investors" in actively traded virtual currency. Currently, the mark-to-market election applies only to "dealers" and "traders" in virtual currency that is treated as an "actively traded commodity."

Background

The IRS treats virtual currency as property.[157] An exchange of properties generally is taxable only if the properties "differ[] materially either in kind or in extent" within the meaning of Treasury regulations section 1.1001-1(a).[158]

In *Cottage Savings v. The United States*, the Supreme Court determined that properties differ materially either in kind or in extent if they "embody legally distinct entitlements," even if the properties are economically equivalent to each other.[159]

It is not at all clear how to apply *Cottage Savings*' "legally distinct entitlements" test to digital assets, because digital assets often bear no legal entitlements at all. As a result, it often is difficult for taxpayers to determine whether onchain transactions are taxable events.

Moreover, in August 2022, Treasury and the IRS issued proposed regulations that, if finalized in their current form, would require "digital asset middlemen" to report "sales" of digital assets on new Form 1099-DA. While a discussion of the proposed regulations is beyond the scope of this report, we are concerned that, so long as there remain significant questions about what types of onchain transactions are taxable

[157] IRS Notice 2014-21
[158] Treasury regulations Section 1001.
[159] *Cottage Savings v. United States*,499 U.S. 554 (1991).

exchanges, market participants are likely to reach conflicting views as to whether they are brokers and which transactions (if any) they are required report.

Below we provide examples of several common types of digital asset transactions that might or might not be taxable exchanges.

Protocol upgrades

In CCA 202316008, which is widely understood to address Ethereum's "Merge," the IRS cited to *Cottage Savings* in concluding that a taxpayer who held a blockchain's native token did not have a taxable exchange by reason of the blockchain's protocol upgrade from proof of work to proof of stake.

Ethereum's Merge, which consisted of who hardforks executed simultaneously in September 2022, was itself the culmination of a broader protocol upgrade that began at least as early as the Beacon Chain hardfork in December 2020.[160] The Beacon Chain hardfork enabled ETH holders to stake their ETH and begin processing "empty" blocks alongside the proof of work Ethereum chain. The Merge required those staking validators to run software accepting transaction data from Ethereum execution clients while original Ethereum clients turned off their mining, block propagation, and consensus logic. As a result of the Merge, Ethereum validators now use a proof of stake consensus mechanism and Ethereum now burns base transaction fees, resulting in an automated dynamic monetary policy.[161]

Protocol developers, application developers, infrastructure providers, and validators worked together to ensure that Ethereum users did not feel the effects of the Merge. For example, web3 wallet providers updated their software so that the "ETH" ticker referred to the proof of stake version and "ETHW" referred to the proof of work version, and the Ethereum Foundation, a Swiss nonprofit that owns the Ethereum trademark and is dedicated to supporting the Ethereum ecosystem, advocated for the adoption of the proof of stake chain.

In short, the Merge represented a significant protocol change that required massive coordination among diverse market participants to minimize disruption to end-users. Nevertheless, CCA 202316008 observes (without explanation) that ETH was "unchanged by the protocol change."

The CCA appears to stand for the proposition that protocol changes, in and of themselves, do not trigger a taxable exchange of the protocol's native token, regardless

[160] It also included the Berlin hardfork in April 2021 and the London hardfork in September 2021.
[161] Very generally, during times of high network throughput, more ETH is burned than minted, reducing aggregate ETH supply, and during times of low network throughput, more ETH is minted than burned, increasing th aggregate ETH supply.

of how significant those changes are. While that proposition seems reasonable in light of *Cottage Savings*' focus on legal entitlements, taxpayers generally may not rely on CCAs as precedent and it is unclear to us how far the CCA extends.

Because protocol upgrades are a commonplace occurrence in web3, we urge the IRS to further study and clarify the circumstances (if any) under which a protocol upgrade should constitute a tax event to tokenholders.

Noncustodial wrapping

Noncustodial wrapping involves depositing one token (such as ETH) into software in exchange for a 1:1 pegged representation of the same token (such as wETH). Users can wrap or unwrap a token by (1) interacting directly with the wrapping software, (2) exchanging the token for its wrapped counterpart on a decentralized exchange, or (3) engaging a transaction that automatically wraps or unwraps a token within a series of actions.

Noncustodial wrapping is very common in web3; as of November 2022, over 7% of all Ethereum transactions, or about 125 million transactions, involved wETH.[162] While most tax practitioners believe noncustodial wrapping transactions are nontaxable, there are no legal authorities directly on point. As mentioned above, *Cottage Savings* treats two properties as materially different in kind or in extent if they have different legal entitlements, and most tokens do not have any legal entitlements.

Custodial wrapping

Custodial wrapping involves depositing a token (such as BTC) with a custodian in exchange for the custodian's agreement to mint a new token contractually backed by the custodied token on a different blockchain (such as wBTC on Ethereum). Custodial wrapping requires the assumption of counterparty risk, whereas noncustodial wrapping requires the assumption of software bug and hacking risk. As of March 23, 2024, there were over $10 billion of wBTC in circulation.[163] However, as with noncustodial wrapping, taxpayers do not have any clear guidance as to whether a custodial wrapping transaction is a taxable event.

[162] See Stephen Tong, Formally Verifying the World's Most Popular Smart Contract (Nov. 18, 2022) ("As of block 15934960 (November 9, 2022), WETH has been in 125,581,756 transactions. This count includes all 'top-level' transactions which call the WETH contract at any point, including via an internal transaction."), https://www.zellic.io/blog/formal-verification-weth/

[163] https://etherscan.io/token/0x2260fac5e5542a773aa44fbcfedf7c193bc2c599.

Liquidity provision

Liquidity provision is a foundational component of much of decentralized finance: liquidity providers contribute tokens to automated software, which other users can interact with in various ways (such as engaging in token exchanges or token borrowings), often for a fee. In exchange for their contribution, liquidity providers typically receive either: (1) transferrable "bailment tokens" that represent the deposited tokens, plus fees streamed directly to their wallets; (2) transferrable tokens that can be redeemed for a portion of the assets (including accrued fees) held inside of the software; or (3) the ability to claim their portion of fees, and to remove their liquidity from the software, from time to time.

The U.S. tax treatment of liquidity provision is unknown. Under one approach, a liquidity provider is treated as engaging directly in the activities of the applicable smart contract. If that approach were adopted, liquidity provision presumably would not be a taxable disposition. Under an alternative approach, the smart contract is deemed to be a tax "person" that is not looked through.[164] If that approach were adopted, liquidity provision presumably would be a taxable disposition. It is also possible that some liquidity provision arrangements are looked through and others are not.[165]

Token borrowing

In a decentralized finance borrowing protocol, users who contribute tokens to software can "borrow" other tokens from the software up to a percentage of the value of the tokens they contributed, and can reacquire tokens identical to the ones they contributed by replacing the borrowed tokens and paying a time-based usage fee.

The U.S. tax treatment of on-chain token borrowing is unknown. Under one theory, token borrowing is an exchange of one token for another, and therefore is a taxable exchange. Under an alternative theory, token borrowing is a deferred exchange of property for identical property and therefore is nontaxable under the same principles that led to the enactment of section 1058. It also is possible that some types of token borrowings are taxable exchanges, while others are not. Again, in the absence of clear guidance, it is highly likely that taxpayers and their advisors will reach conflicting views.

---

[164] See, e.g., Jason Schwartz, Squaring the Circle: Smart Contracts and DAOs as Tax Entities, https://www.friedfrank.com/uploads/siteFiles/Publications/Decentralized%20Autonomous%20Organizations%20_%20Decentralized%20Law.pdf (July 29, 2022) (suggesting some pooled smart contracts might be treated as foreign corporations that are not passive foreign investment companies).

[165] See, e.g., Jason Schwartz, The Latest DeFi Alpha Is Tax-Optimized Staking, https://www.friedfrank.com/uploads/documents/cc68fd4ecd02c64da95a5c0752355f73.pdf (May 25, 2022).

SECTION 2: Provide more comprehensive guidance on the taxation of consensus layer staking

Under current IRS guidance, block rewards rewards are taxed at their fair market value when a miner or staker has dominion and control over them.[166]

A discussion of whether the IRS's position on block rewards represents an appropriate interpretation of the law is outside of the scope of this report. Here we instead express concern that the IRS has not given taxpayers sufficient opportunity to engage with it on determining the proper treatment of block rewards and, as a result, there remains significant uncertainty around ancillary questions.

Background on consensus mechanisms

A blockchain is a peer-to-peer network composed of multiple computers (nodes) running open-source software.[167] Although each node acts independently in its own economic interest, the software's incentives are designed so that an information ledger emerges from the nodes' aggregate actions. The incentives are collectively referred to as a "consensus mechanism."

Although each blockchain has its own design, there are broadly two kinds of consensus mechanisms: proof of work and proof of stake.

In a proof of work network, nodes—known as miners in this context—compete to solve a computational puzzle. The first miner to solve the puzzle gets to propose the next block of data for addition to the ledger. If the proposed data block does not contain any transactions that break the network's rules, like "double-spend" transactions or other falsified information, the other nodes validate the "winning" miner's block. In that event, the winning miner receives "block rewards." On the Bitcoin network, block rewards consist of: (1) newly minted BTC and (2) transaction fees. Newly minted BTC currently represents the majority of mining rewards. Transaction fees are fees users are required to pay to include their transactions in a block. If a miner's block is not approved, the miner will not receive any block rewards and, consequently, will be in a net economic loss position after having incurred real-world resources to solve the computational puzzle.

In a proof of stake network, nodes—known as stakers in this context—lock up, or "stake," a material amount of the blockchain's native token in the software they run. The software selects a staker at random to propose a new block of data for inclusion on the ledger. As with proof of work, the other nodes approve the winning staker's block if it

[166] IRS Notice 2014-21 (mining rewards); Revenue Ruling 2023-14 (staking rewards).
[167] Open-source means the software is free to use, modify, and distribute.

does not contain falsified information, and the winning staker receives block rewards. On the Ethereum network, block rewards consist of: (1) newly minted ETH and (2) "priority gas fees." Newly minted ETH represents the majority of staking rewards. Priority gas fees are fees some users pay in excess of a mandatory "base fee" for faster inclusion in a block. (Unlike Bitcoin, Ethereum's software protocol destroys, or "burns," base fees, thereby offsetting the inflationary effects of newly minted ETH.) If a staker's block is not approved (e.g., because the staker submitted falsified data), all or a portion of the staker's ante is devalued, or "burned."

IRS guidance

The IRS concluded in Notice 2014-21 that "when a taxpayer successfully 'mines' virtual currency, the fair market value of the virtual currency as of the date of receipt is includible in gross income." Similarly, in Revenue Ruling 2023-14, the IRS held that "[i]f a cash-method taxpayer stakes cryptocurrency native to a proof-of-stake blockchain and receives additional units of cryptocurrency as rewards when validation occurs, the fair market value of the validation rewards received is included in the taxpayer's gross income in the taxable year in which the taxpayer gains dominion and control over the validation rewards."

Problems with IRS guidance

While Notice 2014-21 and Revenue Ruling 2023-14 reflect the IRS's views, they are not binding on taxpayers. There are two overarching problems with the IRS's approach of describing the treatment of block rewards through nonbinding guidance.

First, the guidance does not provide sufficient analysis for tax practitioners to assess the IRS' position on its legal merits or to reach conclusions on ancillary matters. As a result, there remains significant confusion by taxpayers and practitioners about whether: (1) non-U.S. persons are subject to U.S. income or withholding tax when they earn block rewards through a U.S. delegate;[168] and (2) block rewards are taxed as "unrelated business taxable income" to U.S. tax-exempt organizations.[169] A regulatory project involving notice and comment would have given taxpayers an opportunity to ask these questions and the IRS an opportunity to respond.

Second, making tax policy through nonbinding administrative guidance rewards taxpayers with sufficient resources to take an alternative position. In *Jarrett v. United*

[168] Very generally, non-U.S. persons are subject to U.S. federal income tax on income effectively connected with the conduct of a trade or business within the United States, and are subject to 30% U.S. federal withholding tax (which may be reduced by an applicable income tax treaty) on U.S.-source fixed, determinable, annual, or periodical income that is not effectively connected with the conduct of a trade or business within the United States.
[169] Very generally, U.S. tax-exempt organizations are subject to U.S. federal income tax on unrelated business taxable income.

States,[170] a home staker sued the IRS for a refund of the tax he paid on his newly minted block rewards, arguing that the rewards were self-created property instead of property received for services. The IRS contested Jarrett's refund suit, then granted his refund and successfully sued to dismiss the case on mootness grounds. The taxpayer's experience in *Jarrett* illustrates that there are currently two tax regimes for consensus-layer stacking: one for taxpayers who can afford to sue the IRS for a refund each year, and one for taxpayers who cannot.

[170] No. 3:21-CV-00419 (M.D. Tenn. 2021).

Article 4: Intellectual Property Considerations in Web3

The migration to Web3 introduces a complex landscape for intellectual property (IP) rights, challenging conventional enforcement mechanisms and necessitating a reevaluation of legal frameworks. This shift is primarily due to the decentralized nature of Web3, where blockchain technology underpins the creation, distribution, and ownership of digital assets.

In Web3, as characterized by its decentralized nature and reliance on blockchain technology, traditional copyright enforcement mechanisms encounter new challenges. The crux of these challenges lies in how digital works—such as art, music, and literature—are managed and transacted on blockchain ledgers. This shift necessitates a reevaluation of conventional copyright concepts, including ownership, distribution, and infringement, within this novel context.

Definition and Overview of NFTs:

Non-Fungible Tokens (NFTs) are unique cryptographic tokens recorded on a blockchain or similar distributed ledger system, providing the owner with rights in or access to one or more assets or entitlements. They offer a way to document ownership and authenticity of digital and physical assets, but also create potential for intellectual property infringement due to their immutable and decentralized nature.

Legal Frameworks and Challenges

Traditional intellectual property laws were not designed with digital assets like NFTs in mind. This means applying these laws can be complex. NFTs essentially represent ownership or proof of authenticity of a digital asset using blockchain technology. The legal challenge is to determine how existing copyright, patent, or trademark laws can govern the ownership, transfer, or licensing of NFTs. These complexities often require rethinking how intellectual property rights are structured in the digital age, considering the decentralized and often international nature of blockchain technology.

SECTION 1: Copyright Considerations in Web3 & for Digital Assets

Under traditional copyright law, copyright is automatically granted to the creator of an original work that is fixed in a tangible medium of expression. This law gives the creator exclusive rights to use, distribute, and reproduce the work, as well as to create

derivative works. Enforcement mechanisms typically involve legal action against unauthorized use or distribution, relying on centralized institutions (such as courts and copyright offices) to adjudicate disputes and enforce rights.

NFTs may impact the minting, storage, marketing, and transfer of digital content, implicating copyright law. They offer possibilities for documenting authorship and enabling digital rights management but raise concerns about enforcing copyright in a decentralized environment.

A. Copyright Challenges with Digital Works

In Web3, works are often recorded on a blockchain—a decentralized ledger that eliminates the need for central authorities. While this enhances security and transparency, it also blurs traditional lines of copyright ownership. For instance, a digital artwork tokenized as a Non-Fungible Token (NFT) might be sold or transferred across the globe without easy recourse to centralized copyright registration systems.

Blockchain technology facilitates the easy and rapid distribution of digital works. Once a work is recorded on a blockchain, it can be copied or transferred without degradation of quality, challenging traditional copyright enforcement mechanisms which rely on controlling the distribution of physical copies.

The decentralized nature of Web3 complicates the detection of copyright infringement. Without centralized platforms monitoring copyright compliance, identifying and addressing copyright violations becomes more difficult. The immutable record of blockchain transactions provides a clear history of asset transfers, but it does not automatically police copyright violations.

Utilizing blockchain technology for digital rights management (DRM) allows creators to embed copyright information directly into the digital work or associated NFT. This can include smart contracts that help automate royalty payments or restrict unauthorized distribution. While restricting unauthorized distribution may be true with respect to NFTs (cryptographic tokens), it is not necessarily true of underlying expressive works, which remain as easy to copy as they were in Web2. Automated royalties have all but disappeared because of vexing technological challenges that would require universal participation by marketplaces to overcome, providing a mechanism for rights enforcement that aligns with Web3's decentralized ethos.

DAOs can offer a community-driven approach to copyright management, where decisions regarding copyright enforcement and dispute resolution are made collectively

by stakeholders. This model could facilitate a more adaptable and responsive copyright enforcement mechanism within the Web3 environment.

The global nature of Web3 and blockchain transactions necessitates international legal cooperation to address copyright challenges. One way to address this could be to develop standardized legal frameworks that recognize and enforce copyright across borders in the digital domains. While these same issues exist currently in the Web2 space, the development and increased use of Web3 seem to make them more pronounced and ripe for further consideration.

SECTION 2: Trademark Considerations in Web3 & for Digital Assets

A. Trademarks in Web3

The application of trademarks in Web3 transcends traditional branding paradigms. In this new environment, digital assets themselves can serve as brand identifiers, challenging the conventional application of trademark law.

Trademarks, traditionally understood as symbols, words, or phrases legally registered or established by use as representing a company or product, face new interpretations and challenges in Web3. Here, digital assets—ranging from digital art to virtual goods—can serve not only as commodities but also as identifiers of brand origin, pushing the boundaries of traditional trademark paradigms.

NFTs present new opportunities for brand extension into digital realms and challenges for trademark registration and enforcement. The USPTO report suggests that while NFTs can enhance brand interaction with consumers, they also increase the risk of trademark infringement on NFT marketplaces.[171]

Traditionally, trademark law serves two primary purposes: it protects the brand identity of companies, ensuring that consumers can distinguish between the products of different producers, and it prevents unfair competition by prohibiting other businesses from using similar marks that could confuse consumers. Trademark protection is typically granted to marks used in commerce that are distinctive and non-functional, with rights established through registration with relevant authorities or through actual use in commerce.

[171] https://www.uspto.gov/sites/default/files/documents/Joint-USPTO-USCO-Report-on-NFTs-and-Intellectual-Property.pdf

B. Trademark Challenges and Adaptations in Web:

In Web3, digital assets like NFTs (Non-Fungible Tokens) and virtual goods become more than just items of trade; they act as brand identifiers. This blurs the lines between product and trademark, as these assets can carry the brand's identity directly within the digital or virtual environment. For example, a unique digital artwork or a specific virtual item might not only be valuable in its own right but also serve to identify its creator or the brand behind it.

The decentralized nature of blockchain and Web3 complicates jurisdictional issues related to trademark protection. Traditionally, trademark rights are territorial, meaning they are protected within the jurisdictions where they are registered or used. However, the global and borderless nature of blockchain technology challenges this principle, as digital assets can be traded and recognized worldwide without clear jurisdictional boundaries.

Enforcing trademark rights in Web3 poses practical challenges. The anonymity of blockchain transactions and the lack of centralized control make it difficult to identify and take action against infringers. Traditional enforcement mechanisms, such as cease and desist letters or litigation, may not be as effective in a decentralized environment where asset holders can be anonymous or spread across multiple jurisdictions.

Given the global nature of Web3, there is a growing need for international cooperation and harmonization of trademark laws to address the challenges of digital asset branding. Developing standardized protocols for the registration, recognition, and enforcement of trademarks across borders could help mitigate some of the jurisdictional challenges posed by Web3.

Legal frameworks may need to evolve to better accommodate the unique aspects of branding in Web3. This could involve rethinking the criteria for what constitutes a trademark, how trademark use is defined in a digital context, and how rights are established and enforced in decentralized networks.

The unique nature of digital assets on blockchain platforms necessitates a rethinking of how trademark law is applied. For instance, the use of a specific digital asset (e.g., a unique piece of digital art or a character in a virtual world) as a brand identifier may require adaptations in trademark law to address issues of distinctiveness, use in commerce, and potential infringement in a decentralized context.

Leveraging smart contracts can offer new ways to enforce trademark rights in Web3. For instance, smart contracts could be programmed to verify the authenticity of a digital asset or enforce licensing agreements automatically, providing a mechanism for protecting trademarks without the need for centralized enforcement.

SECTION 3: NFTs and their intersection with IP Rights

This area presents a complex legal landscape that necessitates a nuanced understanding of both technological and legal principles. NFTs, which certify the unique ownership of digital assets such as artwork, music, or videos on a blockchain, introduce innovative opportunities for creators to monetize and manage the distribution of their works. The discussion revolves around the use of NFTs for managing and licensing patent rights. Although NFTs can facilitate these processes, there are concerns about the precision and reliability of such records on blockchain technologies.[172] These opportunities are accompanied by intricate legal challenges, especially regarding intellectual property rights.

In March 2024, the United States Patent and Trademark Office released a report on the intersection of intellectual property rights and NFTs.[173] Despite the challenges identified in the report, the office concluded that there is no current need to change IP laws to address the use of NFTs.[174]

A. Ownership vs. Intellectual Property Rights

Owning an NFT does not inherently grant the owner the copyright of the digital asset linked to the NFT. This critical distinction underscores the need for clarity about what rights NFT purchasers are acquiring. While the NFT certifies ownership of a unique digital token, the copyright — the legal right to control the use and distribution of the digital content — may still reside with its original creator or a designated copyright holder.

While purchasing an NFT, buyers often receive limited rights to the digital asset associated with the NFT. It's crucial to understand that the ownership of the NFT does not automatically grant ownership of the copyright or trademark associated with the digital asset itself. For example, buying an NFT of a digital artwork does not typically transfer copyright ownership of the artwork; it merely grants the NFT holder some usage

[172] *Id.*
[173] *Id* @72.
[174] *Id.*

rights, which should be clearly defined in the terms of sale. This distinction needs to be clearly communicated to prevent legal issues surrounding digital rights management.

The trading and monetization of NFTs tethered to digital content without proper authorization can lead to significant copyright infringement issues. Creators and sellers must ensure they have the legal rights to the digital content associated with their NFTs. This includes a clear articulation and agreement on the extent of rights being transferred in an NFT transaction to prevent unauthorized use and distribution of copyrighted digital content.

B. Enforceability and Jurisdictional Challenges.

The decentralized nature of blockchain and the global marketplace for NFT transactions introduce formidable challenges in enforcing intellectual property rights. The traditional legal framework, built around territorial jurisdiction, faces hurdles in addressing infringements that occur in a borderless, decentralized digital space. Determining jurisdiction and applicable law for disputes involving NFTs and associated digital content requires innovative legal approaches and potentially new legal doctrines to address the decentralized operations of blockchain technologies.

Enforcing intellectual property rights in a decentralized platform like blockchain presents unique challenges. Traditional enforcement mechanisms often rely on geographical jurisdictions to tackle infringements, but with blockchain, an infringer can be anywhere in the world, and the data related to the infringement is distributed across a global network of nodes. This dispersal complicates the process of identifying, targeting, and taking legal action against infringers or unauthorized uses of digital assets.

Addressing the legal challenges posed by NFTs and IP rights necessitates the development of clear, comprehensive legal frameworks. These frameworks should outline the rights transferred with NFT sales, including any limitations on the use and distribution of the associated digital content.

Given the global nature of NFT transactions, once again, leading us to recognize the pressing need for international legal cooperation and harmonization of laws governing digital assets and intellectual property rights. This includes agreements on jurisdictional principles and enforcement mechanisms that are adaptable to the decentralized, digital nature of NFTs.

Educating creators, collectors, and legal professionals about the intricacies of NFTs and intellectual property rights is crucial. Increased awareness can help prevent unintentional infringements and promote a more legally compliant ecosystem for NFTs.

SECTION 4: Smart Contracts: Legal Status and Enforceability

Although smart contracts are just code deployed to a blockchain, many people mistakenly assume they are necessarily legally binding agreements. They are sometimes designed to supplement or even replace standard legal contracts, and they have the advantage of being self-executing and self-enforcing, without the need for intermediaries, which theoretically reduces costs, increases speed, and enhances trust in transactions.

A. Legal Challenges

Since many in the legal industry are still learning about smart contracts and understanding them, there are often challenges made to their contractual validity. For a smart contract to memorialize the terms of a legally binding agreement, it must meet the traditional criteria of a contract, including offer, acceptance, consideration, capacity, and intention to create legal relations. The digital nature of smart contracts raises questions about how these elements are verified in a code-based environment.

The decentralized nature of blockchain technology leads to smart contracts that incorporate parties across multiple jurisdictions. Given the decentralized nature of blockchain, determining jurisdiction and the applicable law for disputes arising from smart contracts is challenging. The transnational nature of blockchain networks means a smart contract could be executed across multiple legal jurisdictions, complicating legal enforcement.

The enforceability of smart contracts in court depends on the ability of legal systems to recognize and interpret code as binding agreements. Additionally, the immutability of blockchain means that once a smart contract is executed, it cannot be easily amended or revoked, which may conflict with certain legal principles, such as the right to rescind a contract under specific circumstances.

B. Solutions and Adaptations

Some jurisdictions have begun to adapt their legal frameworks to recognize the validity of smart contracts. For example, amendments to electronic transactions laws in some countries explicitly include smart contracts, acknowledging their ability to carry out transactions and agreements.

Currently, New York has a proposed bill which is still in committee which would require that "[S]ignatures and records secured through blockchain technology and smart contracts. 1. a signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature."[175]

Arizona and Tennessee have both passed a law explicitly approving smart contracts.[176] The Arizona law explains the term smart contract as "an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger."[177] It defines a signature or contract "that is secured through blockchain technology" is valid, and, indeed, "may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term."[178] Two other U.S. states have issued laws giving legal recognition to data stored on a blockchain, which may apply also to smart contracts: Nevada, and Vermont[179].

One suggested solution is a hybrid contract that combines traditional written contracts with smart contracts. The written contract outlines the broader terms and legal intentions, [180]while the smart contract executes specific, automatable clauses. This approach can help bridge the gap between legal requirements and technological execution and has been deployed widely in connection with NFT projects.

Another solution that is being explored to address the issues arising with smart contracts are dispute resolution mechanisms. One suggestion is to develop dispute resolution mechanisms, including digital arbitration and mediation, tailored to the digital and decentralized context of smart contracts, is crucial for addressing potential conflicts.

SECTION 5: Development of Trademark/Copyright Infringement Case Law

Hermès Int'l v. Rothchild

The Hermes International v. Rothschild case, otherwise known as the "MetaBirkins" case, illustrates how traditional luxury brands are confronting new digital realities.[181] Hermès sued the creator of MetaBirkins NFTs, which were digital representations of its Birkin bags. Hermès argued that these NFTs infringed upon its

---

[175] https://www.nysenate.gov/legislation/bills/2021/A3760
[176] H.B. 2417, 53d Leg., 1st. Sess. (Ariz. 2017), https://legiscan.com/TN/text/SB1662/2017
[177] H.B. 2417, 53d Leg., 1st. Sess. (Ariz. 2017).
[178] *Id.*
[179] https://www.leg.state.nv.us/Session/79th2017/BDR/BDR79_59-0158.pdf; https://legislature.vermont.gov/statutes/section/12/081/01913
[180]https://neo-project.github.io/global-blockchain-compliance-hub//united-states-of-america/USA-smart-contracts.html#:~:text=As%20of%20that%20date%2C%20Arizona,contracts:%20Nevada%2C%20and%20Vermont
[181] *Hermès Int'l v. Rothschild,* 2023 U.S. Dist. LEXIS 109010, 2023 WL 4145518, at *7 (S.D.N.Y. June 23, 2023)

trademark rights, demonstrating the tension between established IP laws and new digital formats.

In February 2023, Hermès won the lawsuit. The jury found that the NFTs violated Hermès' trademark rights and awarded the company about $133,000 in damages. The judge also issued a permanent ban on the sale of "MetaBirkins" NFTs, saying that continued sales would cause Hermès irreparable harm.[182]

This against Mason Rothschild, the creator of "MetaBirkins" NFTs established a landmark decision. It set a precedent for how physical product trademarks might be protected when represented digitally.

Nike vs. *StockX* LLC

Nike's lawsuit against StockX underscores the conflict between brand owners and new digital marketplaces.[183] Nike alleged that StockX was misleading consumers into buying counterfeit Nike products at inflated prices. StockX denied the allegations and said that it is committed to ensuring the authenticity of all items sold on its platform. Nike took the position that NFTs are products themselves, while StockX's position was that they are receipts for physical products.

The case adds some clarity to how courts treat NFTs and how far third parties can use established brands' trademarks in their own NFTs.

Miramax vs. Quentin Tarantino

This conflict arose when Tarantino announced plans to issue NFTs based on his film "Pulp Fiction," which Miramax argued would infringe on its copyright rights.[184] The case settled out of court upon undisclosed terms.

The case emphasizes the complexities of copyright ownership and control in the era of digital assets, where original creators and rights holders may have conflicting interests regarding how a work is utilized and monetized in new digital formats.

Yuga Labs, Inc. v. Ripps, et al.

In or about May of 2022, Ryder Ripps and Jeremy Cahen launched the Ryder Ripps Bored Ape Yacht Club (RR/ BAYC) collection, a set of NFTs closely resembling Bored Apes, which Ripps claimed were endorsing Nazi codes and symbols. Later in

[182] *Id.*
[183] *Nike vs. StockX LLC,* 22-CV-00983 (S.D.N.Y.).
[184] *Miramax vs. Quentin Tarantino,* 21-CV-08979 (C.D. Cal.).

2022, Yuga sued Ripps, accusing him and his colleague, of manufacturing and selling fake NFTs that undercut the worth of the original pieces.[185] A United States district court judge ordered Ripps and Cahen to pay Bored Ape Yacht Club creator, Yuga Labs, a total of $1.57 million in disgorgement and damages, including legal fees.[186] The matter is up on appeal.

SECTION 6: Blockchain and Real Property Transactions

Blockchain technology offers a secure, transparent, and efficient method for recording and transferring real property rights. Smart contracts, a feature of blockchain, can automate many aspects of real property transactions, including title transfers, payments, and even compliance with legal requirements. This could significantly reduce the time and cost associated with real estate transactions, while also minimizing the potential for fraud.

A. Legal Challenges

Traditionally, real property titles are recorded in public registries operated by governmental entities, providing a legal record of ownership. Integrating blockchain into this process raises questions about the legal recognition of digital titles and the role of government in verifying and recording property ownership.

While smart contracts can automate transactional elements, their legal status in real estate transactions is not fully established. Issues such as the parties' capacity to contract, the formalities required for real property transactions, and the ability to enforce these agreements in courts remain areas of legal uncertainty.

Again the decentralized nature of smart contracts creates jurisdictional issues and questions. Real property is inherently local, subject to the laws and regulations of the jurisdiction where it is located. However, blockchain operates on a global scale, potentially complicating jurisdictional issues in disputes or when enforcing rights.

B. Legal Framework Adaptations for Smart Contracts

1. Legal Recognition of Digital Titles:

Legislators may need to enact laws that recognize digital titles and registrations on a blockchain as legally valid and equivalent to traditional paper titles. This involves

[185] *Yuga Labs, Inc. v. Ripps, et al.,* CV 22-4355 (C.D. Cal.).
[186] https://storage.courtlistener.com/recap/gov.uscourts.cacd.855658/gov.uscourts.cacd.855658.431.0.pdf.

ensuring that digital records meet all legal requirements for real property transactions, including evidence of ownership, encumbrances, and liens.

2. Hybrid Systems:

Implementing a hybrid system that maintains traditional title registration mechanisms while integrating blockchain technology could offer a transitional solution. This approach would leverage blockchain's efficiency and security while retaining the legal framework's established protections and recognitions.

3. Dispute Resolution and Enforcement:

Developing new legal frameworks and dispute resolution mechanisms that can accommodate the decentralized nature of blockchain transactions is crucial. This might include specialized courts or arbitration panels familiar with blockchain technology and real property law.

Article 5: Navigating the Nexus of Emerging Technologies and Criminal Justice: Challenges and Opportunities in the Age of Digital Currencies and Assets

SECTION 1: Introduction

The decentralized and global nature of digital currency and the increased potential for cross border transactions have inspired the need for regulation, legislation, lawsuits, and prosecutions. Initially, most of these cases focused on identifying where these currencies fit into our current financial and regulatory structure, questions regarding ownership, the legality of their use and if there is a need for a new regulatory framework. It was not until recently that the criminal justice communities began to focus on the fraud, criminal enterprises and abuses of digital currency. The *FTX* case brought with it the mainstream recognition of how digital currencies and finance were being used in illegal manners.

Further, our communities have continued to explore the manners in which these currencies can be used to bank the unbankable and improve access to justice and resources. The opportunities for people to hold digital assets in digital wallets have increased as has their use. The unstable nature of these currencies makes them less accepted in countries with stable economies such as the United States for the time being, while those countries with less stable fintech are increasingly incorporating digital currencies into their banking and financial systems. In New York, while we continue to manage the issues created by digital currency in the courts, our regulatory agencies and legislatures are hard at work to provide sensible and clear guidelines for its use.

The impact of emerging technologies on the criminal justice system is vast. Emerging technologies such as digital currencies and assets, blockchain and Web3 have introduced new tools to facilitate crime including fraud, money laundering and schemes to defraud, they also provide technology that can be used to improve access to justice, the criminal justice system and the courts. These technologies provide new means for accessing and tracking information about cases and individuals, investigating cases and defending them, bail, and the courts.[187] This report will touch on both illicit and productive uses, and show the possibilities for the use of blockchain technology, digital assets and crypto currency in our courts and legal communities.[188]

[187] Embley and Graski, *supra* note 1.
[188] *See id.*

Emerging technologies including Web3, blockchain, cryptocurrency and digital assets, have spurred the development of new avenues for crime and illicit activity. In 2023, $24.2 billion was received by illicit addresses. That same year, crypto crime was 0.34% of total on-chain transaction volume.[189] These numbers include funds sent to addresses that have been identified as illicit and funds stolen in crypto hacks.[190] It must be noted that this percentage dropped from 42% in 2022. Interestingly, these numbers are only 1% of the on-chain crypto activity. There are also crypto scams that take place without a blockchain dimension because they occur off-chain.[191]

New York is also the venue for a large amount of other regulatory enforcement litigation arising from crypto, including the recent *Terraform Labs* matter,[192] which recently went to trial where a jury held Terraform Labs, and its founder, liable for "defrauding investors in crypto asset securities."[193]

These enforcement actions are often venued in Federal Court, in New York's Southern District of New York ("SDNY"), as well as criminal matters such as the Mango prosecution arising out of allegations of commodities fraud, commodities market manipulation, and wire fraud in connection with the manipulation on the Mango Markets digital asset exchange.[194] In addition, many of these actions venued in the SDNY have both enforcement aspects, as well as parallel criminal actions.[195] This overlap of enforcement and criminal actions in the SDNY is not limited to the DOJ and SEC. For example, recently KuCoin, a digital asset exchange, was charged by the CFTC with multiple violations of the Commodity Exchange Act (CEA) and CFTC regulations in SDNY.[196] The DOJ also has commenced a criminal action against KuCoin, also pending in the SDNY, with failing to register with the appropriate U.S. government entities and failure to maintain an anti-money laundering database.[197]

To the extent that any of the actions conflict, the Second Circuit and possibly the Supreme Court, will have the final say. Nonetheless, it is evident that crypto related litigation is highly prevalent in New York, both in Federal and New York State Court.[198]

---

[189] The 2024 Crypto Crime Report, Chainalysis, February 2024.
[190] *Id.*
[191] *Id.*
[192] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-32.pdf
[193] https://www.sec.gov/news/statement/grewal-statement-040424
[194] https://www.justice.gov/usao-sdny/pr/man-convicted-110-million-cryptocurrency-scheme.
[195] See, https://www.sec.gov/news/press-release/2023-13; US. V. Wahi https://www.justice.gov/media/1233526/dl; SEC v. Wahi https://www.sec.gov/files/litigation/complaints/2022/comp-pr2022-127.pdf
[196] https://www.cftc.gov/media/10421/enfkucoincomplaint032624%20/download
[197] https://www.justice.gov/media/1345231/dl
[198] See, People of the State of New York v. Vino Global Limited D/B/A Coinex,https://ag.ny.gov/sites/default/files/memorandum_of_law_in_support_of_petition._nyoag_v._vinogloballtd_dba_coinex.pdf

In California, there is a website that *attempts* to keep track of the scams and lists out more than 15 ways to perpetrate crypto scams.[199] Additionally, local FBI offices in California warn of such scams.[200] The latest discussion on cryptocurrency scams from the FTC dated May 2022 is outdated[201] and two years is an incredibly long time in the emerging technology space where changes occur at a much faster rate than any past industry.

The assets that comprise the illicit transactions include Stablecoins, Altcoins, ETH (Ethereum), and BTC (Bitcoin). In 2022 and 2023, the majority of the illicit transactions involved stablecoins.[202] These crime categories included Child Sexual Abuse Material (CSAM), darknet market sales, fraud shops, cybercriminal activities, malware, online pharmacies, scams and transactions with sanctioned entities, scams and transactions operating in sanctioned jurisdictions, scams, stolen funds, special measures, and ransomware extortion.[203] While some illicit crypto activity including darknet market sales and ransomware extortion still operate predominantly in Bitcoin, others, such as scamming and transactions associated with sanctioned entities, now are much more common in stablecoins.[204] Scamming and stolen funds/hacking decreased significantly in 2023, but ransomware and darknet market activity increased. However, it is the transactions with sanctioned entities that have driven the large majority of illicit activity in the crypto currency arena.[205]

Investors are told that they can make quick money by investing in cryptocurrencies, and criminals are fast to attack any vulnerabilities of individuals to exploit them. Fraudulent crypto investment schemes aka “pig butchering” have become commonplace garnering billions of dollars from victims. “Pig butchering,” derived from the concept of fattening a hog before slaughter originated in Asia, but then went global during the pandemic and continues to be a global issue.

Clearly, the evolution of technology has profoundly transformed the landscape of criminal justice, introducing both innovative tools for law enforcement and new avenues for criminal activity.[206] Central to this transformation is the rise of digital currencies and

---

[199] https://dfpi.ca.gov/crypto-scams/
[200] Federal Bureau of Investigation, San Francisco Media Office, “FBI Warns the Public of Holiday Scam Trends,” (Dec. 13, 2023) https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-the-public-of-holiday-scam-trends.
[201] Federal Trade Commission, Consumer Advice, https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams, (last visited Apr. 12, 2024).
[202] *Id.*
[203] *Id.*
[204] *Id.*
[205] *Id.*
[206] Erik Fritzvold, "17 Types of Innovative Police Technology, " https://onlinedegrees.sandiego.edu/10-innovative-police-technologies/ (last visited Apr. 12, 2024).

assets, such as cryptocurrencies, which have posed unique challenges for legal frameworks, law enforcement agencies, and financial regulatory bodies globally.

SECTION 2: Cross-Border Jurisdiction & Collaboration

Cross-border jurisdiction and collaboration have become increasingly important in dealing with cryptocurrency fraud and theft. The decentralized and global nature of digital assets creates many challenges as well. Traditional legal mechanisms often fall short when dealing with anonymous perpetrators and digital assets spread across multiple jurisdictions. However, innovative legal precedents are emerging. In *LCX AG v. John Doe Nos,*[207] the New York Supreme Court allowed for legal documents to be served via NFT airdrops to the wallets involved in a hack. Similarly, the Florida District Court adopted this approach in *Benjamin Arthur Bowen v. Xingzhao Li*[208], authorizing the use of NFT airdrops to serve legal documents to a known fraudster. These cases show how the courts are finding new ways to deal with legal challenges across different jurisdictions by using the same technology upon which digital assets are built. Blockchain technology itself offers unique opportunities for tracking transactions and establishing the provenance of digital assets in ways that were previously impossible, such as the use of NFTs for legal notices.

To address problems with laws across different jurisdictions, we need a comprehensive plan that updates laws, enhances international cooperation, and incorporates new technology into the legal process. In 2021, the DOJ created its National Cryptocurrency Enforcement Team (NCET) tasked "to spearhead complex investigations and prosecution of the criminal misuse of cryptocurrency and to recover illicit proceeds."[209] New York state regulators and federal agencies like the SEC, CFTC, and DOJ through joint task forces and information sharing are creating a unified approach to combat crypto-related crimes. This strategy can streamline investigations, align regulatory efforts, and improve the speed and effectiveness of prosecuting offenders, closing gaps that criminals exploit in the decentralized cryptocurrency market.

Since the foundations of digital currencies often include features such as anonymity and decentralization, which can be exploited for money laundering, fraud, terrorist financing, and other illicit transactions, these collaborations and cross-jurisdiction work is essential. Law enforcement have been working hard to develop

[207] *LCX Ag v. 1.274M U.S. Dollar Coin, No. 154644/2022, 2022 WL 3585277 (N.Y. Sup. Ct. Aug. 21, 2022).*
[208] *Bowen v. Li,* No. 23-CV-20399, 2023 WL 2346292 (S.D. Fla. Mar. 3, 2023).
[209] Brendan J. Harrington et al., *DOJ sharpens its cryptocurrency enforcement focus,* Reuters (Nov. 31, 2021), https://www.reuters.com/legal/transactional/doj-sharpens-its-cryptocurrency-enforcement-focus-2021-11-30/.

specialized knowledge and tools to trace these activities.[210] However, often coordinating cross-border investigations and prosecutions can be a daunting task for authorities.

One of the challenges in cross-jurisdictional collaborations and prosecution is determining the applicable law. The rapid pace of technological change continually alters the cyber-threat landscape. Criminal justice systems struggle to keep legislation and practice in step with technological advancements. Law enforcement must be trained in the collection, preservation, and analysis of digital forensic evidence which requires advanced expertise. The continuous and increasing development of special units within law enforcement agencies for this purpose is proving to be essential in their success in finding and prosecuting bad actors. However, there continues to be significant resource constraints and varying levels of technical capability among agencies tasked with these responsibilities.

Even while facing these challenges, law enforcement has begun to leverage blockchain analysis tools to investigate and map out criminal networks.[211] These tools enable the identification of patterns and ultimately the entities behind illicit transactions. Recent publications highlight successful strategies in combating the operations of Child Sex Abuse Material (CSAM) enterprises.[212] By strengthening international agreements and collaborative efforts, jurisdictions can better combat cyber-enabled financial crimes that exploit digital currencies and assets. Developing comprehensive legal frameworks can provide clear guidelines for the legitimate use of digital assets and effective measures against their misuse. Integrating technology-focused education and training programs within the criminal justice system can help law enforcement to adapt and respond effectively to emerging cyber threats.

Another opportunity not yet being fully embraced is the ability of the courts to use blockchain technology to support their work, securely maintain information, and increase their productivity. In 2018 the National Center for State Courts reported that it was likely that the legal community would see blockchain technology used for court recordkeeping including managing court judgments, warrants, and criminal histories.[213]

SECTION 3: Utilizing Digital Assets for Fraud by Criminal Enterprises

In the ever-evolving landscape of financial technology, cryptocurrencies and Non-Fungible Tokens (NFTs) have emerged as revolutionary instruments of commerce. Alongside their rapid growth and adoption, a parallel and dark narrative unfolds—one

[210] The 2024 Crypto Crime Report, Chainalysis, February 2024.
[211] Chainalysis *supra* note 113.
[212] *Id.*
[213] Embley and Graski, *supra* note 1.

where these digital assets become tools in the arsenal of criminal enterprises.[214] While digital assets offer unprecedented opportunities for economic innovation and freedom, they also open new avenues for fraud and illicit activity.

We need to raise awareness about the use and misuse of emerging technologies as well as educate. Lawyers must remember the ethical challenges and pitfalls that arise when engaging with companies that are using, creating and/or promoting digital currencies and assets.

The rapid evolution and mass adoption of digital currencies create many new challenges and opportunities for legal practitioners. As these financial technologies become increasingly integrated into the global economy, lawyers find themselves navigating a complex landscape shaped by regulatory uncertainties, ethical considerations, and the potential for criminal misuse. Lawyers advising clients in this new and emerging sector must therefore be well versed in Know Your Customer (KYC) and (AML) compliance procedure. The decentralized nature of digital finance and blockchain technology makes it easier than ever to interact with unidentified people or entities. Interacting with unknown customers is a certain path to unintentionally engaging in illicit actions.

KYC regulations are pivotal in the fight against money laundering and terrorism financing. Lawyers working with firms dealing in digital currencies must ensure strict compliance with KYC procedures to verify the identity of their clients and understand the nature of their businesses. This due diligence is essential not only for legal compliance but also for maintaining the integrity of the legal profession and preventing the misuse of digital assets for illicit purposes.

The ethical landscape for lawyers engaging with digital currencies is fraught with potential pitfalls. Unethical behaviors can range from the negligent failure to conduct adequate due diligence to active participation in fraudulent schemes. Lawyers must know that the rules of professional conduct apply and do guide them in these situations, even if they do not specifically use the terms related to the emerging technology space.

Besides ten years in prison, Mark Scott, the lawyer entangled in the

[214] U.S. Department of Justice, Office of Public Affairs, *Justice Department Announces Enforcement Action Charging Six Individuals with Cryptocurrency Fraud Offenses in Cases Involving over $100 Million in Intended Losses,* (Jun. 30, 2022), https://www.justice.gov/opa/pr/justice-department-announces-enforcement-action-charging-six-individuals-cryptocurrency-fraud.

infamous $4 billion Onecoin cryptocurrency fraud had to forfeit to the Southern District of New York a money judgment in the amount of $392,940,000, several bank accounts, a yacht, two Porsche automobiles, and four real-estate properties.[215]

Also, in February 2024, a group of investors embroiled in the FTX mess has filed a lawsuit against Sullivan & Cromwell, accusing it of facilitating the multi-billion dollar fraud in the Southern District of Florida.[216] This case is explored in more depth at the beginning of this report.

The threats posed by the misuse of digital assets are diverse and sophisticated. Much like cash, digital assets can be used by transnational criminal organizations to fuel underground marketplaces for illicit goods, ranging from drugs to illegal weapons. Many criminal enterprises prefer to use cryptocurrencies over fiat currencies to distribute the fruits of their illicit activities due to the perceived anonymity and difficulty in tracing transactions back to their participants. Moreover, digital assets are increasingly utilized to obfuscate the origins of criminally obtained funds, aiding in money laundering, tax evasion, and the evasion of sanctions.

Perhaps most alarmingly, the digital asset space has become fertile ground for fraud schemes directly targeting consumers and investors, including Initial Coin Offering (ICO) ponzi schemes, pig butchering[217] schemes, and rug pulls.[218]

Initial Coin Offering (ICO) Ponzi schemes are fraudulent investment scams promising high returns from digital asset projects, where returns for older investors are paid out from the contributions of new investors, rather than from legitimate business activities.[219]

"Pig butchering" is an internet fraud scheme that primarily targets individuals looking for romantic relationships online. The term is derived from the practice of raising a pig and feeding it until it is ready for slaughter. Similarly, in this scam, the fraudster (also known as the "pig butcher") gains the trust of their victim (the "pig") over a period of time before eventually defrauding them of their money or personal information. The FBI noted in its 2023 Internal Crime Center (IC3) report[220] that “pig butchering” has

---

[215] U.S. District Attorney’s Office, Southern District of New York, “Former Law Firm Partner Sentenced To 10 Years In Prison For Laundering $400 Million of OneCoin Fraud Proceeds,” (Jan. 25, 2024) https://www.justice.gov/usao-sdny/pr/former-law-firm-partner-sentenced-10-years-prison-laundering-400-million-onecoin-fraud.
[216] Garrison v. Sullivan & Cromwell, No. 1:24-cv-20630-XXXX (S.D.Fla. 2024).
[217] *See* Lily Hay Newman, *‘Pig Butchering’ Scams Are Now a $3 Billion Threat,* Wired, (Mar. 9, 2023) https://www.wired.com/story/pig-butchering-fbi-ic3-2022-report/.
[218] *See* Andrew Rossow, *Scams Explained: What are Rug Pulls? Are They a Crime?* nftnow.com, (Oct. 28, 2022) https://nftnow.com/guides/scams-explained-what-are-rug-pulls-and-are-they-a-crime/.
[219] U.S. Securities and Exchange Commission, Office of Investor Education and Advocacy, Investor Alert: Ponzi Schemes Using Virtual Currencies, SEC Pub. No. 153 (7/13).
[220] Internet Crime Report 2022, Federal Bureau of Investigation, 2022, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

overtaken business email compromise (BEC) scams and become the preferred cyber criminal fraud scheme.

In California, there is a website that *attempts* to keep track of the scams and lists out more than 15 ways to perpetrate crypto scams.[221] Additionally, local FBI offices in California warn of such scams.[222] The latest discussion on cryptocurrency scams from the FTC dated May 2022 is outdated,[223] and two years is an incredibly long time in the emerging technology space where changes occur at a much faster rate than in any past industry.

A "Rug Pull" is a deceptive practice in the cryptocurrency space where developers suddenly withdraw all funds from a project and disappear, leaving investors with worthless tokens or digital assets.[224]

Instruments of Deception and Evasion

Blockchain crime is facilitated by several key tools that exploit the inherent features of the technology. Decentralized, un-hosted wallets significantly challenge law enforcement's investigative capabilities, offering criminals a means to operate under the radar. Similarly, certain crypto exchanges and trading platforms lax in enforcing KYC (Know Your Customer) and AML (Anti Money Laundering) regulations, become unwitting accomplices in these schemes. Moreover, phishing attacks and social engineering tactics are rampant, targeting unsuspecting users to siphon off their digital assets. To further complicate matters, crypto mixer and tumbling services can be abused to launder cryptocurrencies, effectively obfuscating the trail of illicit funds.[225]

Dissecting Blockchain Crime

The anatomy of a typical blockchain crime typically follows a three-step process: (1) theft of digital assets, (2) concealment, and (3) launder (or conversion) into fiat currency. This process is facilitated by sophisticated methods such as the use of

[221] California Department of Financial Protection & Innovation, https://dfpi.ca.gov/crypto-scams/, (last visited Apr. 1, 2024).
[222] Federal Bureau of Investigation, "FBI Warns the Public of Holiday Scam Trends", (Dec. 13, 2023), https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-the-public-of-holiday-scam-trends.
[223] Federal Trade Commission, "What To Know About Cryptocurrency and Scams," https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams, (last visited Apr. 1, 2024).
[224] Rosie Perper, *What Is a Rug Pull? How to Protect Yourself From Getting 'Rugged,'* Coindesk, (May 11, 2023), https://www.coindesk.com/learn/what-is-a-rug-pull-how-to-protect-yourself-from-getting-rugged/.
[225] Nikhilesh De, *Crypto Mixers Haven't 'Slowed' DOJ Investigations, Director Says,* Coindesk, (Oct. 11, 2022), https://www.coindesk.com/policy/2022/10/11/crypto-mixers-havent-slowed-doj-investigations-director-says/.

tumblers and mixers, which "tornado" the assets across multiple wallets, making the illicit proceeds difficult to trace and seize.[226]

Notable cases highlight the diverse ways in which blockchain facilitates criminal activity. The infamous Silk Road[227] marketplace illustrated how cryptocurrencies could fuel the sale of illegal goods on an unprecedented scale. The *SamSam ransomware* case[228] and the massive Bitfinex Bitcoin hack[229] demonstrate the critical role of digital assets in ransom and malware schemes, as well as large-scale money laundering. Furthermore, incidents like the Coinbase "insider trading"[230] case and the theft of Seth Green's NFT[231] expose vulnerabilities in trading platforms and the burgeoning NFT market. Each case offers unique insights into the mechanisms of blockchain crime and its far-reaching implications.

Some examples of various fraud schemes include Bitcoin Investment Schemes, Rug Pull Schemes, Pig Butchering Schemes and Romance Schemes.

United States v. Emerson Pires, Flavio Goncalves, and Joshua David Nicholas,[232] offers a classic example of a Bitcoin investment scheme. A global cryptocurrency-based ponzi scheme that generated approximately one hundred million dollars from investors was exposed.[233] EmpiresX, along with the aforementioned, fraudulently promoted itself as a cryptocurrency investment platform and unregistered securities offering. They made numerous misrepresentations regarding a purported proprietary trading bot and fraudulently guaranteed returns to investors and prospective investors in EmpiresX.[234] They then laundered investors' funds through a foreign-based

[226] *See e.g.* U.S. Dep't of the Treasury, Office of Foreign Assets Control, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.
[227] United States Attorney's Office, Southern District of New York, "U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure and Conviction In Connection With Silk Road Dark Web Fraud," (Nov. 7, 2022), https://www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction.
[228] U.S. Department of Justice, Office of Public Affairs, "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," (Nov. 28, 2018) https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.
[229] U.S. Department of Justice, Office of Public Affairs, "Bitfinex Hacker and Wife Plead Guilty to Money Laundering Conspiracy Involving Billions in Cryptocurrency," (Aug. 3, 2023) https://www.justice.gov/opa/pr/bitfinex-hacker-and-wife-plead-guilty-money-laundering-conspiracy-involving-billions.
[230] United States Attorney's Office, Southern District of New York, "Former Coinbase Insider Pleads Guilty In First-Ever Cryptocurrency Insider Trading Case," (Feb. 7, 2023), https://www.justice.gov/usao-sdny/pr/former-coinbase-insider-pleads-guilty-first-ever-cryptocurrency-insider-trading-case.
[231] Eric Mack, *How Scammers Stole Seth Green's Bored Ape Yacht Club NFT and Converted It To Cash,* Forbes, (Jul. 11, 2022), https://www.forbes.com/sites/ericmack/2022/07/11/how-scammers-stole-seth-greens-bored-ape-yacht-club-nft-and-converted-it-to-cash/?sh=156591d61f85.
[232] United States Attorney's Office, Southern District of Florida, "Three Men Charged in $100 Million Cryptocurrency Fraud," (Jun. 30, 2022), https://www.justice.gov/usao-sdfl/pr/three-men-charged-100-million-cryptocurrency-fraud.
[233] *Id.*
[234] *Id.*

cryptocurrency exchange and operated a Ponzi scheme by paying earlier investors with money obtained from later EmpiresX investors.[235]

The facts of The *United States v. Le Ahn Tuan,*[236] display a rug pull scheme. Tuan was involved in the Baller Ape Club, an NFT project that purportedly sold NFTs in the form of various cartoon figures, often depicting apes.[237] The scheme unraveled when they deleted the website, effectively absconding with the investor's money.[238] Tuan and his co-conspirators laundered the stolen funds through "chain-hopping," a method of money laundering in which one type of coin is converted to another. This process involved moving funds across multiple cryptocurrency blockchains and utilizing decentralized cryptocurrency swap services to hide the trail of Baller Ape investors' stolen funds.[239]

The pig butchering scheme exposed in The United *States v. Lu Zhang, Justin Walker and Joseph Wong*,[240] involves three individuals, along with some other co-conspirators, who allegedly defrauded victims of more than $80 million.[241] These scammers targeted victims however they can, be it social media, dating apps, phone calls, phishing, to initiate a relationship.[242] Similar to the romance scheme described below, they built a relationship of trust and then introduced the idea of investing in cryptocurrency for profit.[243] However, once victims began sending money, they were asked for additional funds for fees and further investments, quickly finding themselves unable to retrieve their funds.[244]

In The *United States v. Clinton Chukwudi Uchendu,*[245] Uchendu was found guilty in late March 2024 of participating in a money laundering conspiracy that involved receiving and transmitting funds from victims of romance scams.[246] The conspiracy's objective was accomplished through social manipulators, referred to as "Yahoo Boys," who created fake profiles online, developed relationships with their victims, gained the victim's trust, and then requested money under false pretenses, such as needing money to help a sick child, to assist someone in jail overseas, or being stranded somewhere

---

[235] *Id.*
[236] U.S. Dep't of Justice, Office of Public Affairs, *supra* note 131.
[237] *Id.*
[238] *Id.*
[239] *Id.*
[240] U.S. Department of Justice, Office of Public Affairs, "Four Individuals Charged for Laundering Millions from Cryptocurrency Investment Scams," (Dec. 14, 2023), https://www.justice.gov/opa/pr/four-individuals-charged-laundering-millions-cryptocurrency-investment-scams.
[241] *Id.*
[242] *Id.*
[243] *Id.*
[244] *Id.*
[245] United States Attorney's Office, District of Utah, "Jury Finds Romance Scammer Guilty on All Counts," (Mar. 22, 2024), https://www.justice.gov/usao-ut/pr/jury-finds-romance-scammer-guilty-all-counts.
[246] *Id.*

without access to their bank accounts.[247] Typically operating from Nigeria and pretending to be United States soldiers, international businessmen, or celebrities,[248] the "Yahoo Boys" relied on co-conspirators in the United States, who had US bank accounts to assist them. [249] These individuals referred to as "pickers,"[250] provided accounts to collect funds from the victims and added layers to conceal the source and destination of the funds, thereby avoiding detection by banks[251] As a "picker," Uchendu collected money into bank accounts and then laundered the funds to Nigeria or other destinations.[252]

In response to the escalating use of blockchain crime, government and regulatory bodies have begun to mobilize.[253] The intersection of blockchain technology with criminal enterprises presents a formidable challenge to regulators, law enforcement, and the broader financial community. Understanding the mechanisms of blockchain crime, exemplified through various case studies, is crucial for developing effective strategies to mitigate these risks. As the digital landscape continues to evolve, so too does the responses from governments, regulators, and the crypto community to ensure the integrity and security of the digital economy.

SECTION 4: Criminal Justice Case Law Update

SEC

Recent years have seen major players in the cryptocurrency sector[254], such as Binance, Coinbase, and FTX, face significant legal challenges. These include serious allegations, investigations, and in some cases, complete operational shutdowns. In the absence of direct congressional action, the Securities Exchange Commission has aggressively filled the regulatory void. The SEC's actions have included lawsuits against major exchanges like Ripple, Binance, and Kraken. Amidst these developments, the SEC has also moved forward by approving Spot Bitcoin ETFs.

The *FTX* case is by far the most notable crypto fraud case.[255] In 2017, Sam Bankman-Fried founded his cryptocurrency firm and within just five year, it collapsed.[256]

---

[247] *Id.*
[248] *Id.*
[249] *Id.*
[250] *Id.*
[251] *Id.*
[252] *Id.*
[253] U.S. Department of Justice, "The Report of the Attorney General Pursuant to Section 5(b)(iii) Executive Order 14067: The Role of Law Enforcement In Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets," (Sep. 6, 2022) https://www.justice.gov/ag/file/1557146/dl?inline.
[254] U.S. Securities and Exchange Commission, https://www.sec.gov/spotlight/cybersecurity-enforcement-actions, (last visited Apr. 2, 2024).
[255] *U.S. v. Bankman-Fried,* 2023 WL 5394510 (S.D.N.Y. 2024) (superseding indictment).
[256] *Id.*

The narrative is the same as most of these cases:[257] investor funds were diverted for personal use or to cover other expenses.[258]

The SEC alleged that Bankman-Fried had "from the start" improperly diverted assets that customers had deposited with FTX over to Alameda to fund its trading positions and venture investments.[259] That was in addition to what the SEC said were "lavish real estate purchases and large political donations."[260] As the broader crypto market declined in value through 2022, other lenders began to seek repayment from Alameda.[261] Even though FTX had allegedly already given Alameda billions of dollars in customer funds, the SEC contends that Bankman-Fried began to give Alameda even more money to cover those positions.[262] After being found guilty in the Southern District of New York, Bankman-Fried was sentenced to twenty-five years in prison and eleven billion dollars in forfeiture which is the heftiest sentence yet in a cryptocrime matter.[263]

In December 2020, the SEC filed a lawsuit against Ripple Labs Inc., alleging an illegal $1.3 billion securities offering via XRP sales.[264] [265] Recently, a federal judge denied the SEC's appeal request against a decision favoring Ripple, a significant blow to the regulator's crypto market oversight efforts.[266] The SEC aimed to appeal findings on XRP's "programmatic" sales and other uses as payment, but the judge saw no substantial disagreement warranting an appeal. This decision halts further SEC appeals, emphasizing a critical moment in Ripple's legal battle.

Then in June 2023, the SEC charged Binance with multiple violations including artificially inflating trading volumes, misappropriating customer funds, failing to restrict U.S. customers, and misleading investors about market surveillance controls.[267] Additionally, Binance faces charges for unlawfully allowing the trading of unregistered cryptocurrency tokens.[268]

---

[257] *Id.*
[258] *Id.*
[259] U.S. Securities and Exchange Commission, "SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX," (Dec. 13, 2022), https://www.sec.gov/news/press-release/2022-219.
[260] *Id.*
[261] *Id.*
[262] *Id.*
[263] *Id; U.S. v. Bankman-Fried, 2023 WL 5394510 (S.D.N.Y. 2024) (superseding indictment).*
[264] U.S. Securities and Exchange Commission, "SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering," (Dec. 22, 2020), https://www.sec.gov/news/press-release/2020-338; *Securities and Exchange Commission v. Ripple Labs*, No. 1:20-cv-10832, (S.D.N.Y. 2020), https://www.sec.gov/files/litigation/complaints/2020/comp-pr2020-338.pdf.
[265] https://www.sec.gov/files/litigation/complaints/2020/comp-pr2020-338.pdf
[266] Jonathan Stempel, "US SEC cannot appeal Ripple Labs decision, judge rules," Reuters (Oct. 4, 2023), https://www.reuters.com/legal/us-sec-cannot-appeal-ripple-labs-decision-judge-rules-2023-10-04/.
[267] *Securities and Exchange Commission v. Binance Holding Limited*, No. 1:23-cv-01599, (D.D.C. 2023), https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf.
[268] U.S. Securities and Exchange Commission, "SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao, (Jun. 5, 2023), https://www.sec.gov/news/press-release/2023-101.

Following these charges, Binance CEO Changpeng Zhao admitted to a felony for his failure to prevent money laundering on the platform, resulting in his resignation. [269] The Cayman Islands-based company also acknowledged failures in complying with the Bank Secrecy Act and sanctions programs, particularly in reporting suspicious transactions.

As a result, the U.S. Treasury has subjected Binance to five years of monitoring and stringent compliance requirements to ensure the firm completely exits the U.S. market. Binance agreed to a $4.3 billion settlement with the Department of Justice and the Commodity Futures Trading Commission over breaches related to illicit finance.[270] This agreement is part of a broader settlement which U.S. Attorney General Merrick Garland noted as one of the largest corporate fines in U.S. history.[271]

Further, two Binance employees, American Tigran Gambaryan and Nadeem Anjarwalla, a UK citizen, have been detained in Nigeria, without charges since February 26, 2024.

The SEC charged Kraken in November 2023, by filing charges against Payward Inc. and Payward Ventures Inc., which is collectively known as Kraken, for operating as an unregistered securities exchange, broker, dealer, and clearing agency.[272][273] Earlier, in February 2023, Kraken had agreed to stop offering or selling securities through its crypto asset staking services and programs and consented to pay a $30 million civil penalty.[274]

Supporting Kraken, the Chamber of Digital Commerce submitted an amicus brief, highlighting concerns over the SEC's regulatory reach and calling for clearer regulations in the cryptocurrency sector.[275]

---

[269] United States District Attorney's Office, Office of Public Affairs, "Binance and CEO Plead Guilty to Federal Charges in $4B Resolution," (Nov. 21, 2023) https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.
[270] Hannah Lang and Chris Prentice, *Binance, SEC face off over regulator's crypto oversight,* Reuters, (Jan. 22, 2024), https://www.reuters.com/legal/binance-kicks-off-oral-arguments-push-end-sec-lawsuit-2024-01-22/.
[271] United States District Attorney's Office, Office of Public Affairs, *supra* note 186.
[272] *Securities and Exchange Commission v. Payward, Inc.,* No. 3:23-cv-06003, (N.D.C.A. 2023), https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-237.pdf; U.S. Securities and Exchange Commission, "SEC Charges Kraken for Operating as an Unregistered Securities Exchange, Broker, Dealer, and Clearing Agency," (Nov. 20, 2023), https://www.sec.gov/news/press-release/2023-237.
[273] https://www.sec.gov/news/press-release/2023-237
[274] U.S. Securities and Exchange Commission, "Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay $30 Million to Settle SEC Charges," (Feb 9, 2023), https://www.sec.gov/news/press-release/2023-25.
[275] *Securities and Exchange Commission v. Payward, Inc.,* No. 3:23-cv-06003-WHO, (N.D.C.A. 2024), https://digitalchamber.wpenginepowered.com/wp-content/uploads/2024/02/2024-02-27-Administrative-Motion-dckt-40_2.pdf.

U.S. Department of Justice's Role in Combating CryptoCrime

In 2021, Krstijan Krstic was charged with conspiracy to commit securities fraud, conspiracy to commit wire fraud, and conspiracy to commit money laundering in a cryptocurrency scheme in which he solicited U.S. investors using fraudulent online investment platforms.[276]

The indictment against Kristin is an example of the seriousness being attributed to the cryptocurrency schemes by the IRS Criminal Investigation and the federal law enforcement community.[277] This case is still pending in the Eastern District of New York,[278] and the SEC has also filed a case against him.[279]

In 2022, the Department of Justice announced the release of a comprehensive report and the establishment of a nationwide Digital Asset Coordinator (DAC) Network.[280] These initiatives are in response to the President's Executive Order on Ensuring Responsible Development of Digital Assets, emphasizing the department's commitment to curbing the illicit use of digital technologies that threaten the American public's security and financial stability. Attorney General Merrick B. Garland underscored the necessity of collaborative efforts across government agencies to mitigate crimes facilitated by digital assets while promoting responsible innovation and maintaining national security. The report highlights the criminal misuse of digital technologies and outlines regulatory and legislative recommendations to enhance law enforcement capabilities in this domain.

As a result of the DOJ's increased focus on cryptocurrency crime, a number of recent high-profile prosecutions have followed.

On Jan. 31, 2023, DeMarr, 55, of Santa Ana, California, the former Director of North American Operations for Start Options and B2G, was sentenced to five years in prison for his role in the scheme.[281] His indictment said that the proceeds from the

---

[276] U.S. Department of Justice, Office of Public Affairs, "Leader of $70 M Cryptocurrency and Binary Options Fraud Schemes Extradited to U.S.," (Nov. 3, 2023), https://www.justice.gov/opa/pr/leader-70m-cryptocurrency-and-binary-options-fraud-schemes-extradited-us.

[277] United States District Attorney's Office, Eastern District of New York, "Founder of International Cryptocurrency Companies Indicted in Multi-Million Dollar Securities Fraud Scheme," (Feb. 23, 2021), https://www.justice.gov/usao-edny/pr/founder-international-cryptocurrency-companies-indicted-multi-million-dollar-securities.

[278] *Id.*

[279] *United States District Attorney's Office, Northern District of Texas, "United States v. Kristijan Krstic, Et Al.", (last visited Apr. 2, 2024), https://www.justice.gov/usao-ndtx/united-states-v-kristijan-krstic-et-al.*

[280] United States Department of Justice, Office of Public Affairs, "Justice Department Announces Report on Digital Assets and Launches Nationwide Network," (Sep. 16, 2022), https://www.justice.gov/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network.

[281] *United States District Attorney's Office, Eastern District of New York, "U.S. Promoter of Foreign Cryptocurrency Companies Sentenced to 60 Months in Prison for His Role in Multi-Million Dollar Securities Fraud Scheme," (Jan. 31, 2023), https://www.justice.gov/usao-edny/pr/us-promoter-foreign-cryptocurrency-companies-sentenced-60-months-prison-his-role-multi.*

scheme were used for lavish things for himself including the purchase of a Porsche, jewelry, and the remodeling of his home in California.[282]

In May 2023, former OpenSea employee, Nathaniel Chastain, was found guilty after trial for his role in an NFT “insider trading” wire fraud and money laundering prosecution.[283]

In July 2023, Alexander Mashinsky, founder and CEO of Celsius Network (Celsius), has been charged with orchestrating a fraudulent scheme to deceive customers about the true state of the company's affairs. Furthermore, he's alleged to have inflated the price of Celsius's native token, CEL.[284]

In November 2023, former founder of FTX, Sam Bankman Fried, was convicted of two counts of wire fraud conspiracy, two counts of wire fraud, and one count of conspiracy to commit money laundering.[285] That same year, Binance’s founder and chief executive officer (CEO), Changpeng Zhao, pleaded guilty to failing to maintain an effective anti-money laundering (AML) program, in violation of the Bank Secrecy Act (BSA) and resigned as CEO of Binance.[286]

In December 2023, Russian national Anatoly Legkodymov, pled guilty in a federal court in Brooklyn to operating a money transmitting business in connection with Bitzlato Ltd., a crypto exchange.[287]

In yet another similar case, “IcomTech” and “Forcount” were both alleged cryptocurrency mining and trading companies that promised to earn investors profits in exchange for their purchase of purported cryptocurrency-related investment products.[288]

---

[282] *Id.*
[283] U.S. District Attorney’s Office, Southern District of New York, “Statement of U.S. Attorney Damian Williams On The Conviction of Nathaniel Chastain” (May 3,, 2023) https://www.justice.gov/usao-sdny/pr/statement-us-attorney-damian-williams-conviction-nathaniel-chastain.
[284] U.S. Attorney’s Office, Southern District of New York, “Celsius Founder and Former Chief Executive Officer Charged In Connection With Multibillion-Dollar Fraud And Market Manipulation Schemes,” (Jul. 13, 2023) https://www.justice.gov/usao-sdny/pr/celsius-founder-and-former-chief-revenue-officer-charged-connection-multibillion#:~:text=Today%20I%20am%20announcing%20the,a%20scheme%20with%20Celsius%27s%20Chief.
[285] U.S. District Attorney’s Office, Southern District of New York, “Statement of U.S. Attorney Damian Williams On The Conviction of Samuel Bankman-Fried” (Nov. 2, 2023) https://www.justice.gov/usao-sdny/pr/statement-us-attorney-damian-williams-conviction-samuel-bankman-fried.
[286] United States Department of Justice, Office of Public Affairs, “Binance and CEO Plead Guilty to Federal Charges in $4B Resolution,” (Nov. 21, 2023) https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.
[287] U.S. Attorney’s Office, Eastern District of New York, “Founder And Majority Owner of Cryptocurrency Exchange Pleads Guilty to Unlicensed Money Transmitting,” (Dec. 6, 2023) https://www.justice.gov/usao-edny/pr/founder-and-majority-owner-cryptocurrency-exchange-pleads-guilty-unlicensed-money.
[288] *United States District Attorney’s Office, Southern District of New York, “U.S. Attorney Announces Fraud and Money Laundering Charges Against The Founders and Promoters of Two Cryptocurrency Ponzi Schemes,” (Dec. 14, 2022), https://www.justice.gov/usao-sdny/pr/us-attorney-announces-fraud-and-money-laundering-charges-against-founders-and-promoters.*

But, once again the money was diverted to the co-conspirators. They were prosecuted by the U.S. Attorney Damian Williams in an effort to send a message to all cryptocurrency scammers that they will be prosecuted for such illicit actions. The prosecution displays a collaboration between federal, state, and international law enforcement."[289] "IcomTech" and "Forcount" were found guilty March 15, 2024, on one count of conspiracy to commit wire fraud and are awaiting sentencing later this year.

In February 2024, Letitcia James, the Attorney General of New York filed an amended complaint against Gemini Trust Company (Gemini), Genesis and DCG for misleading investors about an investment program called Gemini Earn causing over $3 billion in losses.[290]

In March 2024, Roman Sterlingov, a 33-year-old Swedish-Russian national, was convicted by the Department of Justice (DOJ) of laundering $336 million through Bitcoin Fog, a bitcoin mixing service aimed at obscuring the origins of cryptocurrency transactions.[291]

The founders of KuCoin, Chun Gan and Ke Tang were indicted in the Southern District of New York in March 2024.[292] Since its founding in the fall of 2017, KuCoin has become one of the largest global cryptocurrency exchange platforms.[293] They were charged with Conspiracy to Violate the Bank Secrecy Act and Conspiracy to Operate an Unlicensed Money Transmitting Business and also Operation of an Unlicensed Money Transmitting Business and Violation of the Bank Secrecy Act.[294] It is alleged that they willfully failed to maintain an adequate AML program and thus allegedly allowed billions of dollars in illicit funds to be laundered.[295] This interestingly has had an effect on investment and pig butchering scams as those scammers have been unable to access some of their funds on KuCoin.[296]

Child Sexual Abuse Material Scams

Unfortunately, in the last few years, CSAM (child sexual abuse material) scams have expanded and become more difficult to detect by using digital currency and

[289] *Id.*
[290] *The People Of The State Of New York v. Gemini Trust Company, LLC et al., 0452784/2023, https://ag.ny.gov/sites/default/files/2024-02/genesis-amended-complaint.pdf*.
[291] U.S. District Attorney's Office, District of Columbia, "Jury Finds Russian-Swedish Operator of 'Bitcoin Fog' Guilty of Running the Darknet Cryptocurrency Mixer" (Mar. 12, 2024) https://www.justice.gov/usao-dc/pr/jury-finds-russian-swedish-operator-bitcoin-fog-guilty-running-darknet-cryptocurrency.
[292] United States Attorney's Office, Southern District of New York, "Prominant Global Cryptocurrency Exchange KuCoin and Two Of Its Founderrs Criminally Charged With Bank Secrecy Act and Unlicensed Money Transmission Offenses," (Mar. 26, 2024) https://www.justice.gov/usao-sdny/pr/prominent-global-cryptocurrency-exchange-kucoin-and-two-its-founders-criminally.
[293] *Id.*
[294] *Id.*
[295] *Id.*
[296] *Id.*

blockchain. There is an increase in websites that use crypto currency to sell child abuse material.[297] These currencies include Bitcoin, Ethereum, Dogecoin, Litecoin and Solana.[298] Payments can be made for specific pieces of material or for subscriptions. The Internet Watch Foundation (IWF) has dedicated its work to tracking and identifying bad actors and websites related to CSAM. In 2022, in response to an increase in reports of websites containing crypto information and requests for information from law enforcement, the crypto unit was developed. The IWF works to identify and remove the bad content from the networks, while also assisting law enforcement by providing alerts and access to the data and information it collects. A recent and ongoing collaboration between New York City, South Carolina, Jacksonville Florida and the Philippines resulted in multijurisdictional prosecutions of members of a CSAM scheme in the Philippines. The case is still ongoing.

SECTION 5: Congress's Role in the Pursuit of Bad Actors

The SEC maintains that the majority of cryptocurrency assets qualify as "investment contracts" under the Securities Act of 1933, thereby falling within its regulatory scope. However, the approach of classifying digital assets as securities and the subsequent regulation by the SEC has faced backlash within the crypto industry and from other regulatory bodies, arguing that the SEC's application of the criteria from the landmark SEC v. W.J. Howey Co case is misapplied.[299]

The U.S. Supreme Court's "Howey test," which was established in 1946 and has long been a key means for classifying securities and determining whether an asset constitutes an investment contract.[300] For decades, U.S. courts have applied the test in discerning the line between securities and non-investments; however, the adaptability of the "Howey test" and similar legal standards has been scrutinized in its application to cryptocurrencies.

Under Howey and subsequent case law, an "investment contract" exists when there is: (1) the investment of money, (2) in a common enterprise, (3) with a reasonable expectation of profits, (4) to be derived from the efforts of others.[301] The four-part Howey test was intended to apply to any contract, scheme, or transaction, regardless of

[297] The International Centre for Missing & Exploited Children and Standard Chartered, "Cryptocurrency and the Trade of Online Child Sexual Abuse Material," (Feb. 2021), https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf.
[298] Chainalysis *supra* note 113.
[299] John Deaton, "SEC Crypto Litigation Ventures Into Dangerous Legal Territory," Bloomberg, (May 2, 2023), https://news.bloomberglaw.com/us-law-week/sec-crypto-litigation-ventures-into-dangerous-legal-territory.
[300] *SEC v. W.J. Howey Co*., 328 U.S. 293 (1946).
[301] *Id*. *See also United Housing Found., Inc. v. Forman*, 421 U.S. 837 (1975); *Tcherepnin v. Knight*, 389 U.S. 332 (1967); *SEC v. C. M. Joiner Leasing Corp.*, 320 U.S. 344 (1943).

whether it has any of the characteristics of typical securities.[302] Additional guidance from the Securities and Exchange Commission has suggested additional relevant considerations in applying the Howey test to digital assets.[303]

Some Congressional members have criticized the SEC's actions on crypto, suggesting that the agency should obtain Congressional approval before targeting alleged wrongdoers. They argue that cryptocurrencies should be treated more like commodities, placing them under the Commodity Futures Trading Commission's (CFTC) purview. [304]

Moreover, the SEC's stance on crypto assets diverges from the interpretations of other agencies. For instance, the CFTC identifies certain crypto assets like Bitcoin, Ether, and Litecoin as commodities.[305] The Internal Revenue Service (IRS) treats digital assets as property,[306] while the Financial Crimes Enforcement Network (FinCEN) categorizes it as a virtual currency. [307] Additionally, former SEC Chair Jay Clayton has stated that crypto assets designed as alternatives to sovereign currencies should not be regarded as securities, aligning his perspective more closely with other agencies rather than the SEC's current stance.[308]

The variance in regulatory interpretation of digital assets underscore the difficulty in establishing clear oversight in the absence of a robust regulatory framework. As a result, federal agencies have navigated this landscape through their rulemaking processes. However, these agency-determined jurisdictions over digital assets might face critical examination under the major questions doctrine by courts. Historically, the U.S. Supreme Court has shown deference to agency rules, but recent decisions

---

[302] Under the *Howey* test, "form [is] disregarded for substance and the emphasis [is] on economic reality." *Id*. at 298. The Court further explained that that the term security "embodies a flexible rather than a static principle" in order to meet the "variable schemes devised by those who seek the use of the money of others on the promise of profits." *Id*. at 299.

[303] Securities and Exchange Commission, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets, (last visited Apr. 2, 2024).

[304] Fatima Hussein and Ken Sweet, "Regulators and law enforcement crack down on crypto's bad actors. Congress has yet to take action," Associated Press, (Nov. 22, 2023), https://apnews.com/article/binance-crypto-ftx-defi-blockchain-969377e746bbd1538ab5cbc988a490e4.

[305] Stephen M. Humenik, et al., Client Alert, "CFTC and SEC Perspectives On Cryptocurrency and Digital Assetes–Volume I: A Jurisdictional Overview," (May 6, 2022), https://www.klgates.com/CFTC-and-SEC-Perspectives-on-Cryptocurrency-and-Digital-Assets-Volume-I-A-Jurisdictional-Overview-5-6-2022.

[306] Internal Revenue Service, *Internal Revenue Bulletin: 2014-16*, (Apr. 14, 2014), https://www.irs.gov/businesses/small-businesses-self-employed/digital-assets#:~:text=IRS%20Notice%202014%2D21%20%E2%80%93%20guides,to%20transactions%20using%20virtual%20currency.

[307] Financial Crimes Enforcement Network, "FinCEN Proposes New Regulation to Enhance Transparency in Convertible Virtual Currency Mixing and Combat Terrorist Financing," (Oct. 19, 2023), https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency.

[308] Roger E. Baron et al., "Are cryptocurrencies securities? The SEC is answering the question," Reuters, (Mar 21, 2022), https://www.reuters.com/legal/transactional/are-cryptocurrencies-securities-sec-is-answering-question-2022-03-21/.

demonstrate a shift, particularly when an agency asserts significant regulatory authority over important economic and political matters without clear precedent. This is pertinent to the SEC classifying most crypto assets as "investment contracts," thus placing them under their jurisdiction. This move could be interpreted as the agency asserting substantial regulatory power over the cryptocurrency market. The SEC's use of the "Howey Test" for determining whether crypto assets are securities could invoke the major questions doctrine. This expansive interpretation has paralleled other regulatory scenarios that have prompted the Supreme Court to apply the major questions doctrine.[309]

To address the regulatory ambiguity and jurisdictional disputes, proposed legislation should aim to define clearly which agencies are responsible for regulating different aspects of the industry. This includes establishing more objective criteria for when and how crypto assets should move between regulatory regimes.

Current State of Crypto Regulation in the US Congress

The regulation of crypto assets is increasingly being recognized as a matter of significant political importance. Over fifty bills and resolutions concerning digital asset regulation have been introduced in Congress.[310] Moreover, there is a notable bipartisan consensus in the US Congress focused on addressing crypto crime.[311] Lawmakers across party lines are collaborating to pass legislation targeting the illegal activities connected to digital assets.[312]

SECTION 6: Legislative Initiatives to Combat Illicit Actors

Digital Asset Anti-Money Laundering Act/DAAMA

The Digital Asset Anti-Money Laundering Act, initially presented at the end of 2022 and reintroduced in 2023 by a bipartisan group of U.S. Senators, aims to align the cryptocurrency sector with the existing anti-money laundering regulations of the traditional financial system.[313] This Act seeks to extend the requirements of the Bank

[309] Daniel Kuhn, "Why Binance, Coinbase, Ripple, and Other Crypto Firms Cite the 'Major Questions' Doctrine During Legal Imbroglios," Coindesk, (Oct 17, 2023), https://www.coindesk.com/consensus-magazine/2023/10/17/why-binance-coinbase-ripple-and-other-crypto-firms-cite-the-major-questions-doctrine-during-legal-imbroglios/.
[310] Jason Brett, "Congress Has Introduced 50 Digital Assets Bills Impacting Regulation, Blockchain, and CBDC Policy," Forbes (May 19, 2022), https://www.forbes.com/sites/jasonbrett/2022/05/19/congress-has-introduced-50-digital-asset-bills-impacting-regulation-blockchain-and-cbdc-policy/?sh=4321c7564e3f.
[311] Allyson Versprille, "Fighting Crypto Crime Is One Thing Both US Political Parties Agree On," Bloomberg, (Feb. 13, 2024), https://www.bloomberg.com/news/newsletters/2024-02-13/fighting-crypto-crime-is-one-thing-both-us-political-parties-agree-on?embedded-checkout=true.
[312] *Id.*
[313] S. 2669, 118th Cong. (2023-2024).

Secrecy Act (BSA), including Know-Your-Customer (KYC) protocols, to various participants including wallet providers, miners, and validators. The goal of the 2023 Act is to ensure that these "crypto participants" adhere to the same regulatory standards as traditional financial institutions. If the bill passes, these entities will be required to submit reports for transactions exceeding $10,000 and disclose any suspicious activities that might indicate money laundering or tax evasion.[314] Furthermore, the bill stipulates that any U.S. resident holding over $10,000 in cryptocurrency in foreign accounts must report these holdings to the FinCEN.

Terrorist Financing Prevention Act of 2023

Introduced by a bipartisan team of U.S. Senators, this legislation aims to extend sanctions to foreign organizations that support US-designated terrorist groups, including through cryptocurrency transactions.[315] This act is intended to block Foreign Terrorist Organizations and their financial supporters, who utilize digital assets, from accessing the U.S. financial system. The act enforces sanctions and stringent regulations to deter such activities.

Responsible Financial Innovation Act

Also, introduced by a bipartisan team of Senators, Kristan Gillabrand and Cynthia Lummis continue to work as a team to regulate the US Crypto Industry. The first version of this bill was introduced in June 2023 and the most recent version of the bill was introduced at the beginning of 2024. The 2024 Bill is known as the “Lummis-Gillabrand Responsible Financial Innovation Act.”[316] After the fall of FTX and other big litigations, their newest version puts a focus on consumer protection. The first section of the proposed bill is titled “Putting Consumer Protection First.”[317] The bill has eight additional substantive sections which include handling of illicit finance, commodities regulation, securities regulation, “Customer Protection and Market Integrity Authority”, taxation, interagency coordination, and “Equipping Agencies to Protect Consumers and Promote Responsible Innovation.”[318] Certain parts of the parts of the Bill tend to be getting the most attention including requiring companies to segregate client assets and impose third party custody requirement, requiring companies to show that their reserves can cover customer balance, its creation of new advertising standards for marketing cryptocurrency, and defining “decentralized crypto asset exchange” for the first time. By requiring mandatory registration with the Commodities Futures Trading Commission

[314] Casey Wagner, “Dueling crypto anti-money laundering bills face off in the Senate,” Blockworks, (Aug 7, 2023), https://blockworks.co/news/dueling-crypto-anti-money-laundering-bills.
[315] S. 3441, 118th Cong. (2023-2024).
[316] S. 4356, 117th Cong. (2021-2022).
[317] *Id.*
[318] *Id.*

(CFTC) for crypto asset exchanges, it would give the CFTC primacy over the Securities and Exchange Commission (SEC) when it comes to the crypto spot market. Algorithmic stablecoins would be regulated by the CFTC. If the Bill passes, it will require that payment stablecoins can only be issued by a bank or credit union.

Currently, the Lummis-Gillabrand Bill has not been adopted. However, it seems to have a promising future. Representative French Hill, vice chair of the House Financial Services Committee and chair of the Subcommittee on Digital Assets stated:

> "I am glad to see Senators Lummis and Gillibrand reintroduce their bipartisan legislation to establish a regulatory framework for digital assets. Their work demonstrates that protecting consumers, providing legal clarity, and spurring innovation was never a partisan effort. I look forward to our continued work with our Senate colleagues on common sense legislation."

The ongoing debate that seems to be delaying much of this regulation is whether the Federal Government should be the primary regulatory body for crypto and digital asset regulation or of there should be some combination with state officials. Similar issue exists between the SEC and CFTC. As it currently stands, it appears that the two bills that seem to be moving in the House are a Stablecoin Bill and the Market Structure Bill. From the Senate the Lummis-Gillabrand Bill is certainly sparking discussion.[319]

Committee Actions in the House

The House Financial Services Committee recently made a decisive move by voting to advance a resolution aimed at rejecting the Securities and Exchange Commission's Staff Accounting Bulletin 121 (SAB 121).[320] This guidance has sparked controversy for mandating that financial institutions include customers' cryptocurrency assets in their balance sheets.

In addition, the committee voted unanimously to advance the Combating Money Laundering in Cyber Crime Act.[321] This act aims to bolster the US Secret Service's authority over criminal activity involving digital assets.[322]

---

[319] Kristin Gillibrand, Press Release, July 12, 2023.
[320] Nikhilesh De and Jesse Hamilton, "U.S. House Panel Votes to Disapprove of Controversial SEC Custody Guidance," Coindesk, (Feb. 29, 2024), https://www.coindesk.com/policy/2024/02/29/us-house-panel-seems-poised-to-disapprove-of-controversial-sec-custody-guidance/.
[321] H.R. 7156, 118th Cong. (2023-2024).
[322] Sarah Wynn, "House Finance Committee votes to move forward with measure to overturn SEC's custody bulletin," The Block, (Feb. 29, 2024), https://www.theblock.co/post/280000/house-finance-committee-votes-to-move-forward-with-measure-to-overturn-secs-custody-bulletin.

Despite these initiatives and ongoing discussions, Congress has not yet enacted specific measures to regulate crimes involving cryptocurrencies.[323] Lawmakers are grappling with the task of defining cryptocurrencies while actively pursuing legislative measures to enhance AML standards, combat crypto crime, and safeguard national security The bipartisan support and ongoing efforts reflect a shared commitment to addressing the challenges posed by illicit activities involving digital assets.

SECTION 7: Use of Blockchain To Assist the Criminal Justice System

Blockchain technology can be used to maintain court records and criminal history databases. Since blockchain is an immutable ledger that offers greater security and broader access, it is a better and more accurate resource than a central server. It is more secure and accurate when managing court judgements, record keeping, criminal histories and pending matters. There also exists great opportunities to use blockchain technology to reduce mass incarceration.[324] Blockchain can be used for record keeping, maintaining police disciplinary data systems, and to create uniform statewide pre-trial data collection.[325]

The increased focus on wrongful convictions in the United States combine with its incredibly high incarceration rate in the world. In 2022, the United States housed almost two million prisoners[326] which was twenty percent of the global prison population.[327] Incarcerated people often "lose" their court and legal documents and/or do not have access to them. Further, there is more and more focus on transparency of information. New York's discovery laws mandate the release of disciplinary information of law enforcement as part of the discovery process in all criminal cases.[328]

The evaluation of technology has allowed the storage of almost all discovery digitally. Furthermore, discovery in New York's criminal justice system and many other states is transferred between law enforcement, legal entities and attorneys electronically with it being stored digitally. Blockchain technology has the ability to provide secure storage of discovery, court files, legal files and police records. By using blockchain technology in this manner, our courts, attorneys, law enforcement and other agencies can provide the ability to securely share information. Blockchain offers "real-time

[323] Sam Brown and Erika Kelton, "We need new laws to combat crypto crimes," The Hill, (Aug. 22, 2023), https://thehill.com/opinion/technology/4163374-we-need-new-laws-to-combat-crypto-crimes/.
[324] Maria Rojas, "Modernizing Justice: Implementing Blockchain Technology Into the Criminal Justice System to Reduce Mass Incarceration," 47 Vill. L. Rev. 200 (2023), https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2450&context=lr/.
[325] *Id.*
[326] *See* ACLU, "Mass Incarceration," http://www.aclu.org/issues/smart-justice/mass-incarceration (last visited Apr. 12, 2024)(identifying constitutional violations v. Constitutionality of new legislation or regulations.
[327] Rojas, *supra* note 241.
[328] N.Y. Crim. Proc. Law § 245.

immutable record-keeping".[329] Its decentralized nature allows it to connect through algorithms amongst a network of connected computers. Use of this technology will decrease the expense of cloud storage large amounts of data in multiple locations and provide ease of access while significantly reducing the need to transfer large volumes of data. It would also reduce the amount of time needed to manually maintain data. For example, "participants in the disposition of those criminal charges - including prosecutors, courts and criminal-history repositories - would update the single [b]lockchain records with the action [taken]."[330] Blockchain technology offers broader access with greater security.

Blockchain technology also has promising implications for promoting personal finance skills and enhancing cryptocurrency knowledge among prisoners, in turn, facilitating their re-entry into the increasingly tech-driven workforce following their release. For example, a cryptocurrency called CellBlocks is working to digitize major prison economies to make inmate financial transactions safer, more reliable, transparent, and consistent. If implemented successfully, CellBlocks would be the world's first decentralized cryptocurrency to penetrate the United States carceral system. This technology would not only enable inmates to exchange money without the risk of violence, exorbitant fees, or theft by prison administrators, but also, it would keep an immutable blockchain network record of every transaction circulating in the prison system, thereby reducing the risk of corruption or fiscal impropriety. Projects like CellBlocks serve as a promising avenue to expand inmate financial literacy and acquisition of crypto/blockchain skills to promote successful reintegration into society after serving their sentence."[331]

This promise does not come with concern–in particular concerns over the potential security hazards of giving prisoners internet access to access cryptocurrency and blockchain resources.[332] This concern, however, has not stopped other countries from giving their incarcerated individuals real-time access to the Internet–seemingly without compromising public safety.[333] For example, Belgium has made the platform "Prison Cloud" available–which provides incarcerated people with limited and monitored internet access to content including games, books, and legal materials.[334] Similarly, Finland and Denmark provide inmates with limited internet access through their open

[329] Embley and Graski, *supra* note 1.
[330] *Id.* at 30.
[331] Sophia Scott, "Blockchain Behind Bars: The Case for Cryptocurrency in Criminal Justice," Harvard Technology Review, (Aug. 28, 2021) https://harvardtechnologyreview.com/2021/08/28/blockchain-behind-bars-the-case-for-cryptocurrency-in-criminal-justice-2/.
[332] *Id.*
[333] *Id.*
[334] *Id.*

prisons (jails with minimal security), which have some of the world's lowest recidivism rates.[335]

Use of Digital Currency for Bail

Blockchain technology and digital currency have introduced novel possibilities in various sectors, and the realm of criminal justice, including bail procedures, is no exception. The traditional bail system often involves large sums of money, intermediaries, and can be riddled with inefficiencies and corruption. The integration of blockchain and digital currency proposes a system that could be more transparent, secure, and efficient.

The use of crypto and blockchain extends beyond law enforcement and is also utilized as a tool for advocating social change for marginalized communities historically disadvantaged by the criminal justice system.[336] For instance, over 70% of Americans in local jails are awaiting trial and presumed innocent but are detained due to the bail system.[337] This system requires defendants to pay a judge-determined fee to await trial outside jail. Those unable to afford bail remain incarcerated, allowing wealthier individuals to avoid jail time for the same alleged crimes that lower-income individuals face.[338]

The deep-rooted racial wealth gap in the United States, stemming from centuries of systemic oppression and discrimination, exacerbates disparities in the bail system, leading to disproportionately higher incarceration rates among people of color.[339] In response to this issue, Bail Bloc was established. This initiative encourages users to download the Bail Bloc app, allowing them to contribute their computer's spare processing power to mine the cryptocurrency Monero.[340] The mined Monero is then converted to U.S. dollars on a monthly basis, with all proceeds donated to non-governmental organizations that support bail funds within the National Bail Fund Network.[341] This innovative approach provides a means to financially assist individuals who cannot afford their bail fees, ultimately working to address the inequities in the bail system.[342]

---

[335] *Id.*
[336] *Id.*
[337] *Id.*
[338] *Id.*
[339] *Id.*
[340] *Id.*
[341] *Id.*
[342] *Id.*

When applied to bail transactions, blockchain could have the following potential advantages:

Using blockchain as part of the bail system could make for a transparent system and allow real-time monitoring of bail payments. This may allow those monitoring the system to catch any mundane errors currently made when paperwork is not sent in a timely manner. [343]

Due to the cryptographic nature of blockchain, its immutability offers an added level of security against retroactive changing of records. This security, in turn, can also defend against fraud and verify bail money is properly used.

Digital currencies will lower the barrier to posting bail–giving people easier access to their assets to post bail in addition to the process of actually posting bail. Additionally, this is beneficial to those who do not have access to traditional financial services, such as those in custody. As a result, transaction fees associated with bail payments may be significantly decreased through bypassing the traditional banking system and decrease the time of custody attributed to slow transaction times.

For international defendants, the benefits are even more significant. Cross-border payment is generally a transaction that requires time. Digital currencies can simplify the bail process across borders by avoiding currency exchange issues. A blockchain bail system may allow law enforcement to track the origin of bail proceeds–ensuring they are not coming from a criminal enterprise.[344]

When analyzing the use of digital currencies for bail, we must also consider the challenges that must be addressed:

The value of many digital currencies can be highly volatile. A bail amount set at the time of the hearing could fluctuate by the time it's paid, creating complications. Many jurisdictions, including New York, have yet to establish clear legal frameworks for accepting digital currency for government-related payments, including bail. While blockchain provides enhanced security, digital wallets and exchanges have been vulnerable to hacks and theft, which could pose risks for bail transactions.

Thus, the use of blockchain technology and digital currency in the context of bail has the potential to transform the way criminal justice systems operate by offering transparency, security, and efficiency. As with any emerging technology, there are

---

[344] https://balboabailbonds.com/blog/bitcoin-for-bail-bonds/

hurdles to overcome, particularly in regulation and adoption. However, with proper implementation and safeguards, blockchain and digital currency could markedly improve the bail process.[345]

SECTION 8: Money Laundering

Money laundering as discussed below can occur in traditional financial systems or it now occurs in more sophisticated laundering through the blockchain. Today, crypto criminals will utilize bridges and mixers to help facilitate the movement of illicit funds. Crypto mixers, also known as crypto tumblers, are services that offer enhanced transactional privacy by mixing coins from different sources after a transaction. In addition, a blockchain bridge connects two separate blockchain networks. The primary purpose of these bridges is to facilitate the transfer of tokens and data from one blockchain to another. The emergence of smart contract-enabled bridges could also enhance the automation and security of asset transfers.

Traditional Mechanisms, Cryptocurrency Challenges, and Regulatory Evolution

Money laundering is a financial crime that generally stems from the movement of ill-gotten gains associated with other criminal offenses, such as wire fraud. This association primarily exists because money laundering involves making illegally obtained proceeds (i.e., "dirty money") appear legal ("clean"). Understanding this relationship requires dissecting how money laundering is not a standalone offense but is deeply tied to the initial crimes generating illicit proceeds.

The Connection Between Money Laundering, Theft Crimes, and Wire Fraud Generation of Illicit Proceeds

Theft crimes, including wire fraud, are primary sources of illicit proceeds subject to money laundering. Wire fraud, under 18 U.S.C. § 1343, involves using electronic communications to execute a scheme to defraud or obtain money under false pretenses. The proceeds from such crimes often need to be laundered to enter the financial system without raising suspicion.

Layering through Money Laundering

Once the proceeds are obtained through crimes like wire fraud, money launderers use various methods to conceal the funds' origin, ownership, and control.

---

[345] *Id.*

Title 18 U.S.C. §§ 1956 and 1957 outline the legal framework for combating money laundering, focusing on the concealment of proceeds from a specified unlawful activity.

Integration into the Financial System

The ultimate goal of money laundering is to reintegrate the laundered money into the economy, making it appear as legitimate income. This process often involves sophisticated financial maneuvers, including using financial institutions to facilitate the movement of criminally derived property.

The Role of Cryptocurrency and Blockchain in Money Laundering:

Although money laundering crimes are overwhelmingly facilitated by the movement of cash, cryptocurrency and blockchain technologies, the decentralized nature of digital currencies have introduced new dimensions to money laundering, complicating efforts to trace and combat these crimes.

In today's global financial landscape, combating money laundering and ensuring customer due diligence are critical priorities for regulatory bodies and financial institutions. For member firms operating within the securities industry, the Financial Industry Regulatory Authority (FINRA) has established stringent guidelines to address these concerns. One of the key regulations is FINRA Rule 3310[346], which focuses on anti-money laundering (AML) and know your customer (KYC) compliance.

The BSA[347], officially known as the Currency and Foreign Transactions Reporting Act, was enacted by the United States Congress in 1970 as the first significant legislation to combat money laundering. The Act was designed to deter criminal activity by requiring financial institutions to maintain records of cash purchases and report certain transactions.

In 2013, the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Treasury, declared that "administrators or exchangers" of virtual currency qualify as money services businesses (MSBs) under the BSA and FinCEN regulations. According to FinCEN's guidance document, an "exchanger" is defined as a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An "administrator" is a person or entity engaged as a business in issuing a virtual currency and who has the authority to redeem such currency.[348]

---

[346] FINRA Rule 3310 (effective May 11, 2018).
[347] Office of the Comptroller of the Currency, “Bank Secrecy Act,” https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html (last visited Apr. 12, 2024).
[348] Financial Crimes Enforcement Network, Guidance on Application of FinCEN’s Regulations to Persons Administering Exchanging, or Using Virtual Currencies, FIN-2013-G001 (2013).

The BSA requires all MSBs, including those that exchange or transmit virtual currencies, to register with FinCEN. This requirement extends to any "person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency." This means that cryptocurrency intermediaries, such as exchanges and wallet providers, are subject to the same regulatory requirements as traditional financial institutions.

An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person. FinCEN's regulations define the term "money transmitter" as a person that provides money transmission services, or any other person engaged in the transfer of funds. The term "money transmission services" means "the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[349]

In 2020, FinCEN further clarified that the anti-money laundering (AML) requirements placed on other MSBs also applied to "decentralized finance" (DeFi). DeFi refers to blockchain-based finance that removes central authorities like banks and exchanges. Despite the decentralized nature of DeFi, there is a growing movement among U.S. government regulatory bodies to seek stricter BSA, AML and KYC compliance.[350]

Section 80603, of the 2021 Infrastructure Investment and Jobs Act[351] expands the definition of a digital asset broker. Due to the significant impact that this legislation would have on the digital asset sector, implementation has been delayed in order to afford the IRS and U.S. Treasury sufficient time to come up with compliance and enforcement strategies.[352] Once finalized, Section 80603 will require digital asset brokers to impose strict KYC and IRS reporting requirements for digital asset transfers.

Anonymity and Global Reach

Much like cash, cryptocurrencies offer a level of anonymity that makes them an attractive option for laundering the proceeds of criminal conduct. Critics argue that the pseudonymous nature of crypto makes it an appealing vehicle for money laundering

---

[349] *Id.*
[350] United States Department of Treasury, “Illicit Finance Risk Assessment of Decentralized Finance,” (Apr. 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.
[351] H.R. 3684, 117th Cong. (2021).
[352] Infrastructure Investment and Jobs Act of 2021, Pub. L. No. 117–58, §80603 (2021), https://www.irs.gov/pub/irs-drop/a-23-02.pdf.

because it frustrates law enforcement's ability to track the movement of illicit funds. However, these critics often fail to acknowledge that the fully transparent nature of blockchain ledgers also affords criminal investigators an invaluable tool for tracking the movement of illicit funds.

Decentralization

The decentralized nature of blockchain technology presents challenges for regulatory and law enforcement agencies because traditional financial monitoring systems are ill-suited to keep up with the speed and ease with which crypto moves between parties. In response to these challenges, some lawmakers argue that existing anti-money laundering (AML) laws need to be expanded to apply to cryptocurrency transactions. The existing AML procedures for tracking and identifying parties in traditional financial transactions do not mesh well with the decentralized ethos of crypto. Until legislatures come up with practical rules for monitoring and tracking crypto transactions, we will remain stuck in a climate of enforcement and regulatory uncertainty that threatens the continued growth of the decentralized finance (DeFi) sector in the United States.

Money Laundering and Cryptocurrency and Blockchain Technologies

Title 18 U.S.C. §§ 1956 and 1957 define and penalize various forms of money laundering conduct relating to both the domestic and international movement of illicit funds affecting interstate commerce in the United States.[353] Title 18 U.S.C. § 1957 focuses on transactions involving criminally derived property over $10,000, emphasizing the involvement of financial institutions in facilitating the movement of property with knowledge that it was the fruit of criminal conduct.

Title 18 U.S.C. § 1956 primarily focuses on the laundering of monetary instruments and engages with a broader scope of money laundering activities than § 1957. It criminalizes the conduct of financial transactions with proceeds generated from specified unlawful activities, with the intent to promote the carrying on of specified unlawful activity[354]; conceal or disguise the nature, location, source ownership, or control of the proceed of a specified unlawful activity[355]; avoid transaction reporting requirements under state and federal law[356]; international laundering of monetary

[353] 18 U.S.C. §§ 1956, 1957 (2024).
[354] This includes any financial transaction that uses proceeds from unlawful activities to further or support those or other unlawful activities.
[355] This clause targets efforts to make illicit gains appear legitimate, addressing the core of what many consider traditional money laundering.
[356] This is aimed at those who structure transactions in a manner that evades the detection mechanisms established by regulatory authorities, such as breaking up large amounts of money into smaller, less suspicious amounts (often referred to as "smurfing").

instruments[357]; and engaging in transactions involving property derived form unlawful activities[358].

Furthermore, § 1956 also includes provisions for sting operations, allowing for undercover law enforcement actions to catch money launderers in the act, and it introduces severe penalties for violations, including substantial fines and imprisonment.

SECTION 9: Racketeer Influenced and Corrupt Organizations Act's (RICO) Application to Digital Currency

The Racketeer Influenced and Corrupt Organizations Act (RICO) was initially introduced by Congress "to deal with organized crime and the Mafia," and to create "new criminal penalties and civil actions against individuals engaging in certain criminal activities related to an enterprise."[359] The statute addresses two main concerns today: "(1) the infiltration or control of an enterprise by criminals and (2) the operation of an enterprise for a criminal purpose."[360] "[A]lmost fifty years after RICO's passage, criminals are turning to the internet and cryptocurrencies to establish a new frontier for organized crime."[361] "[C]riminals continue to use cryptocurrencies to mask their identities in modern digital twists on classic organized crimes, including money laundering, drug sales, and extortion."[362] RICO is likely broad enough to cover digital currency.

A few cases, both criminal and civil, "have attempted prosecution of cryptocurrency criminals under RICO. In 2017, a grand jury indicted Alexandre Cazes under RICO for his leadership of a criminal enterprise overseeing a massive illegal online marketplace, ten times larger than Silk Road. However, the prosecution ended after Cazes committed suicide. In late 2018, Michael Terpin, a cryptocurrency investor, used RICO to sue a hacker for illegally accessing his phone account and subsequently stealing over twenty-three million dollars in cryptocurrency. Both cases used the operation subsection of the statute."[363]

---

[357] Section1956 also specifically addresses the transfer of funds internationally with the intent to promote specified unlawful activities or to conceal the proceeds of such activities.
[358] It includes transactions involving the proceeds from criminal activities without the requirement that the transaction aim to conceal those proceeds, merely that the transaction involves significant amounts of money derived from criminal conduct.
[359] Andrew Robert Klimek, *Reinvesting in RICO with Cryptocurrencies: Using Cryptocurrency Networks to Prove RICO's Enterprise Requirement*, 77 Wash. & Lee L. Rev. 509 (2020). Available at: https://scholarlycommons.law.wlu.edu/wlulr/vol77/iss1/9
[360] *Id*.
[361] *Id.*
[362] *Id.*
[363] *Id.*

> "In light of the broad applicability of RICO, the DOJ created requirements for authorizing the use of RICO that limit its use. Any prosecution of cryptocurrency criminals must satisfy these requirements:
>
> [A] government attorney should seek approval for a RICO charge only if one or more of the following requirements is present:
>
> 1. RICO is necessary to ensure that the indictment adequately reflects the nature and extent of the criminal conduct involved in a way that prosecution only on the underlying charges would not;
>
> 2. A RICO prosecution would provide the basis for an appropriate sentence under all the circumstances of the case in a way that prosecution only on the underlying charges would not;
>
> 3. A RICO charge could combine related offenses which would otherwise have to be prosecuted separately in different jurisdictions;
>
> 4. RICO is necessary for a successful prosecution of the government's case against the defendant or a codefendant;
>
> 5. Use of RICO would provide a reasonable expectation of forfeiture which is proportionate to the underlying criminal conduct;
>
> 6. The case consists of violations of State law, but local law enforcement officials are unlikely or unable to successfully prosecute the case, in which the federal government has a significant interest;
>
> 7. The case consists of violations of State law, but involves prosecution of significant or government individuals, which may pose special problems for the local prosecutor."[364]

These factors help to ensure that RICO is only used when necessary.[365] However, these requirements for the use of RICO in criminal prosecutions create a barrier for civil complainants using cryptocurrencies to support their RICO cases. Civil RICO plaintiffs in a majority of circuits must allege that they suffered an 'investment injury' resulting from the investment or use of the proceeds in the enterprise to establish standing.[366] The fluctuating cryptocurrency markets make it difficult for plaintiffs to show the

[364] *Id.*
[365] *Id; See,* U.S. Dep't of Justice, Justice Manual § 9-110.310 (2020).
[366] *Id.*

connection between a criminal's use of a cryptocurrency and "an injury that is concrete and particularized enough to allow standing."[367]

Due to the incredibly broad nature of the RICO statute. "Perhaps the true question of whether to employ RICO should be based on whether a particular case reflects Congress's original concern with organized crime."[368] "RICO can be put to good use to protect the cryptocurrency industry when someone engages in an organized and systematic criminal effort to abuse and infiltrate a cryptocurrency network."[369]

Conclusion

Is there a need for new Criminal Statutes to combat these new technologies? In a nutshell, no. Criminals will always evolve along with the new technologies. Currently, there are plenty of statutes to enforce against these cases: Violation of the Bank Secrecy Act, Wire, Bank and Mail Fraud, the money laundering statutes, 18 U.S.C. §§ 1956 and 1957, terrorism laws, prohibition of unlicensed money transmitting businesses, etc.

Emerging technologies and digital currencies bring forth a complex array of issues for the criminal justice system. These technologies offer both new methods for criminals to carry out their activities and innovative tools for legal systems to respond to such challenges. Meeting these challenges requires a dynamic, multifaceted approach that balances the privacy rights of individuals with the imperatives of law enforcement. It also necessitates international collaboration, an adaptable legal framework, and a commitment to continuously develop the forensic and investigative capabilities of criminal justice professionals. Only through such an approach can society hope to stay ahead of criminals who seek to exploit these new technologies for illicit purposes.

[367] *Id.*
[368] *Id.*
[369] *Id.*

Article 6: Ethics/Education

SECTION 1: Attorneys Receiving Advanced Fees in Cryptocurrency

Initially, it should be noted that all lawyers are mandated to keep abreast of changes in technology. RPC 1.1 comment [8] states,

> [t]o maintain the requisite knowledge and skill, a lawyer should (i) keep abreast of changes in substantive and procedural law relevant to the lawyer's practice, (ii) keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information, and (iii) engage in continuing study and education and comply with all applicable continuing legal education requirements under 22 N.Y.C.R.R. Part 1500.[370]

With the rise in popularity of various cryptocurrencies and NFTs, it appears that state and local bar associations have been repeatedly asked to opine as to whether it is permissible for attorneys to accept cryptocurrencies as a form of payment for legal services provided. Based on the holdings of these advisory opinions, accepting cryptocurrency is generally permissible as long as the New York State Rules of Professional Conduct ("RPC") are not violated. However, when accepting cryptocurrency for advanced payment, RPC1.8 (a) and RPC 1.5 (a) are especially important and involve additional layers of complexity, as accepting advanced payment might be viewed as entering into a business relationship with a client.

Changes in how attorneys accept payment are not a new issue. As ethics opinions from the NYSBA have stated, lawyers may allow their clients to pay for legal services by credit card provided:

> (i) the amount of the legal fee is reasonable; (ii) the lawyer complies with the duty to protect the confidentiality of client information; (iii) the lawyer does not allow the credit card company to compromise the lawyer's independent professional judgment on behalf of the client; (iv) the lawyer notifies the client before the charges are billed to the credit card and offers the client the opportunity to question any billing errors; and (v) in the event of any dispute regarding the lawyer's fee, the lawyer attempts to resolve all disputes amicably and promptly and, if applicable, complies with the

[370] N.Y. Rules of Prof'l Conduct R.1.1 cmt. 8 (2017).

fee dispute resolution program set forth in 22 N.Y.C.R.R. Part 137.[371]

In May 2023, the American Bar Association issued guidance regarding advanced payments for legal fees, not limited to digital assets, when it released a Formal Opinion dated May 3, 2023, titled Fees Paid in Advance for Contemplated Services.[372]

Initially the May 3, 2023, opinion explains that advanced fees and retainers are two different methods of payment.[373] While for the purposes of the article the terms "advanced fee" and "retainer" are used interchangeably, the May 2023 Formal Opinion seeks to distinguish the two by stating that a retainer should not be construed as a "payment for the performance of services, but rather is compensation for the lawyer's promise of availability … (and) is not an advance deposit against future legal services."[374]

These differences should be further investigated if attorneys enter into such agreements. Lawyers must understand when the fee becomes the property of the lawyer and when the fee is earned, including transactions involving cryptocurrency. One important aspect to keep in mind is that lawyers must not commingle a lawyer's earned funds with advance deposits. While not in the context of legal representation, the conviction of Sam Bankman-Fried, the founder of the now defunct crypto exchange FTX Trading Ltd., commonly known as FTX, commingled customers' cryptocurrency leading to trouble.

SECTION 2: Applicable Ethical Rules

Generally, according to Part 1200 of the New York State Rules of Professional Conduct, payments in cryptocurrency and NFTs can implicate various ethical rules. However, the payment of lawyer fees via cryptocurrency primarily seems to invoke two particular ethical obligations. Initially, under RPC 1.5(a), there is a prohibition against charging unreasonable fees.[375] Next, and far more nuanced, the acceptance of digital assets as payment may also implicate RPC 1.8(a), which governs the rules pertaining to the improper conflicts of interest that can arise when an attorney enters into a business transaction with a client.[376]

---

[371] New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 1258 (2023)(citing N.Y. State 1050 ¶5 (2015)); *See also* New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 1248 (2022)(It has been recognized for nearly a half century that lawyers may accept credit card payments for legal services. In N.Y. State 362 (1974), we concluded: "The use of credit cards to pay for legal fees is an innovation which should not be discouraged where the participating lawyer complies with the appropriate safeguards . . . [because] it fills a need for a segment of the public that conceivably might not otherwise have access to legal services." Among the necessary safeguards are the protection of clients' confidential information).
[372] A.B.A. Formal Op. 505 (2023).
[373] *Id.*
[374] *Id.*
[375] N.Y. Rules of Prof'l Conduct R.1.5(a) (2017).
[376] N.Y. Rules of Prof'l Conduct R.1.8(a) (2017).

According to RPC 1.5(a) “Fees and Division of Fees,” a fee is considered excessive when, after a review of the facts, a reasonable lawyer would be left with a definite and firm conviction that the fee is excessive.[377] The factors to be considered in determining whether a fee is excessive include: the time and labor required; the novelty and difficulty of the questions involved; the skill requisite to perform the legal service properly; the likelihood, if apparent or made known to the client, that the acceptance of the particular employment will preclude other employment by the lawyer; the fee customarily charged in the locality for similar legal services; the amount involved and the results obtained; the time limitations imposed by the client or by circumstances; the nature and length of the professional relationship with the client; the experience, reputation and ability of the lawyer or lawyers performing the services; and whether the fee is fixed or contingent.[378]

In short, under RPC 1.5, a fee cannot be excessive or unlawful.

Furthermore, Rule 1.8(a), “Current Clients: Specific Conflict of Interest Rules,” states:

> A lawyer shall not enter into a business transaction with a client if they have differing interests therein and if the client expects the lawyer to exercise professional judgment therein for the protection of the client, unless:
>
> (1) the transaction is fair and reasonable to the client and the terms of the transaction are fully disclosed and transmitted in writing in a manner that can be reasonably understood by the client;
>
> (2) the client is advised in writing of the desirability of seeking, and is given a reasonable opportunity to seek, the advice of independent legal counsel on the transaction; and
>
> (3) the client gives informed consent, in a writing signed by the client, to the essential terms of the transaction and the lawyer’s role in the transaction, including whether the lawyer is representing the client in the transaction.[379]

In sum and substance, according to RPC 1.8(a), if the agreement between the client and the attorney is a business transaction, the attorney has to follow additional steps to ensure compliance with the rules.

---

[377] N.Y. Rules of Prof'l Conduct R.1.5(a) (2017).
[378] *Id.*
[379] N.Y. Rules of Prof'l Conduct R.1.8(a) (2017).

SECTION 3: Ethics Opinions

In 2017, Nebraska's Lawyer's Advisory Committee issued Opinion No. 17-03, allowing payment in digital currencies but noting that bitcoin is "not actual currency" so it cannot be deposited into a client trust account.[380] Nebraska's treatment of cryptocurrency as property rather than currency remains a common treatment by bar associations across the country. While this opened the door to applying a "barter currency" analysis as outlined in Connecticut's Informal Opinion 15-04 (exploring a modern barter exchange membership), later opinions have followed Nebraska's approach.[381]

In 2019, the New York City Bar Association ("NYCBA") issued an opinion addressing the question of whether these ethics rules might come into play if, and when, cryptocurrency is used to pay attorney fees.[382] As per the NYCBA opinion,

> [t]he threshold question under Rule 1.8(a) is whether a lawyer and client (or prospective client) are entering into a (i) 'business transaction;' (ii) where the lawyer and the client have differing interests; and (iii) the client expects the lawyer to exercise professional judgment on the client's behalf in the transaction. If so, the lawyer must meet the procedural requirements in the rule.[383]

This is an extremely fact-specific analysis that must be conducted on a case-by-case basis, which emphasizes the complexities and complications that can arise when holding cryptocurrency as a form of advanced payment.

The NYCBA further notes that cryptocurrency is currently treated more like property as opposed to currency. Just as a lawyer and client would be required to negotiate over several deal-points in an agreement for the lawyer to accept some other form of nonmonetary property (e.g. "a piece of land, a painting or a vehicle") in exchange for legal services – which is clearly indicative of a business transaction subject to Rule 1.8(a) – they would be mandated to negotiate to resolve the questions arising from a cryptocurrency transaction.[384]

---

[380] Neb. Lawyers Advisory Committee Formal Op. 17-03 (2017).
[381] Ct. Bar Ass'n Informal Opinion 15-04 (2015).
[382] N.Y. City Bar Ass'n Formal Op. 2019-5 (2019).
[383] *Id.*
[384] *Id.*

If RPC 1.8(a) is triggered, it imposes various requirements before the lawyer can enter into the transaction.[385] The fee must be reasonable in light of the totality of the circumstances. Importantly, according to the NYCBA's opinion, just because a fee is neither excessive nor illegal does not necessarily mean that it is fair and reasonable because Rule 1.8(a) imposes a more demanding standard. Next, the requirement is whether the lawyer has disclosed the terms of the transaction to the client in a manner that can be "reasonably understood" by the client, which will obviously depend on the complexity of the transaction and sophistication of the client. As such, counsel must be very careful when drafting this disclosure and not necessarily rely on standard form language used in other matters.[386]

An ethics opinion from February 2, 2022, which was adopted on September 19, 2022, by Virginia's Supreme Court and authored by the Virginia Bar Association, states that a client's payment of an advance fee using cryptocurrency has the material elements of a business transaction with the client, subject to the requirements of Rule 1.8(a).[387]

Importantly, the D.C. Bar Association stated that Rule 1.8(a), and similar to Rule 1.5(a), requires a lawyer to adequately disclose the terms and implications of the fee arrangement, which must be reasonable. In addition, a lawyer who enters into a business relationship with a client must provide the client with written disclosure of the terms of the agreement, and a reasonable opportunity to confer with independent counsel, and must acquire from the client written, informed consent to the agreement.[388] Furthermore, Rule 1.8(a) adds an independent ethical responsibility to ensure that the fee arrangement is not only reasonable, but also fair to the client.[389]

The Virginia Bar Association, citing to the D.C. Bar Association's suggestions, provides illustrative examples of useful language and topics to include in the disclosure to the client, namely:

> a lawyer accepting cryptocurrency should consider including a clear explanation of how the client will be billed (i.e., in dollars or cryptocurrency); whether and how frequently cryptocurrency held by the lawyer will be calculated in dollars, or otherwise trued-up or adjusted for accounting purposes and whether, upon that accounting, market increases and decreases in the value of the cryptocurrency triggers obligations by either party; how responsibility for payment of cryptocurrency transfer fees (if any) will be allocated; which

[385] *Id.*
[386] *Id.*
[387] Virginia Bar Ass'n, Op. 1898 (2022); *see also* North Carolina Bar Ass'n, Formal Op. 5 (2019); District of Columbia Bar Ass'n, Op. 378 (2020); N.Y. City Bar Ass'n Formal Op. 2019-5 (2019).
[388] District of Columbia Bar Ass'n, Op. 378 (2020).
[389] *Id.*

> cryptocurrency exchange platform will be utilized to determine the value of cryptocurrency upon receipt and, in the case of advance fees, as the representation proceeds (i.e., as fees are earned) and upon its termination; and who will be responsible if cryptocurrency accepted by the lawyer in settlement of the client's claims loses value and cannot satisfy third party liens.[390]

Echoing similar concerns, the Maryland Bar Association held that a lawyer may accept cryptocurrency as payment as long as it complies with the Maryland Attorneys' Rules of Professional Conduct ("MARPC"). Given the nature of cryptocurrency and its attendant inability to be deposited into an Attorney Trust Account, the opinion highlights that alternative fee arrangements involving the receipt of fees paid in cryptocurrency raise a host of potential ethical considerations. Any attorney considering such an arrangement must comply with the entirety of the MARPC.[391]

The Maryland Committee on Ethics further emphasized that just as an attorney might be disciplined for depositing a client's retainer paid in fiat currency into their personal account, which is an example of commingling as discussed above, or the firm's operating account, an attorney who accepts a cryptocurrency retainer could be subject to discipline for succumbing to a phishing attack, for losing access to the digital wallet holding the funds, or mistakenly sending funds to be disbursed back to the client to the wrong address.[392] Because the cryptocurrency industry is mostly unregulated, uninsured, anonymous, and irreversible, it is particularly important for lawyers to appropriately safeguard the cryptocurrency retainer against theft, loss or mishandling, or other similar risks.[393]

As referenced above, the theory behind alternative payment options for attorneys is far from novel. It is very similar to a situation where a party wishes to pay for legal services by tendering stock (which could fluctuate in value over time). One solution might be for the parties to agree that the amount being tendered for advance payment would be calculated as of the time the payment is made, in which case there would be a sharing of potential risk. If the crypto is not liquidated upon payment and goes down in value, the attorney would lose out versus receiving a sum which turns out to be in excess of the expected payment. That might be an irreconcilable conflict of interest and is just one example of how such an arrangement can be problematic.

As mentioned above, while this article specifically discusses RPC 1.5 (a) and 1.8(a), other possible ethical issues highlighted by the NYCBA's ethical opinion in a footnote which might be triggered by accepting cryptocurrency as payment might

---

[390] Virginia Bar Association, Op. 1898 (2022).
[391] Maryland State Bar Ass'n Committee on Ethics, Op. 2022-01 (2022).
[392] *Id.*
[393] *Id*.

include: "(1) whether, and how, a lawyer may properly hold cryptocurrency in trust either for the client or for the benefit of third parties (see Rule 1.15); (2) whether the lawyer has the proper cybersecurity protections and technology controls to maintain cryptocurrency and safeguard against outside attacks (see Rule 1.1); and (3) whether the lawyer and the client have complied with all state and federal laws related to cryptocurrency including, but not limited to applicable criminal laws regulating securities and anti-money laundering laws (see Rules 1.2(d); 8.4(a))."[394]

SECTION 4: Other Ethical Issues

Recently, a former partner at U.S. law firm Locke Lord was sentenced to 10 years in prison for his role in a nearly $400 million fraudulent cryptocurrency scheme, according to Manhattan federal prosecutors. The attorney was found guilty of conspiracy to commit money laundering and conspiracy to commit bank fraud in November 2019, stemming from his role in the OneCoin cryptocurrency fraud.[395]

While this matter involved crypto, attorneys breaking the law and laundering money is nothing new. It merely emphasizes the need to recognize that attorneys will face ethical dilemmas when practicing law, and thus, the bar needs to be prepared.

SECTION 5: Digital Finance and Currency Legal Education in New York State

New York law schools have started taking steps to educate their students about the emerging legal landscape of cryptocurrency and distributed ledger technology ("DLT"):

- *Cornell* has offered "Starting a Crypto Fintech: Legal Roadmap and Case Studies;" "Advanced Writing: Fintech, Alternative Finance and Digital Assets du Jour;" "Crypto Assets and Web3;" and "NFTs: Legal and Business Considerations."[396]
- *Cornell Tech* offers a Master of Laws (LLM) in Law, Technology, and Entrepreneurship.[397]
- *Hofstra* offers "Global Fintech Law and Policy," which provides a "general overview of the evolving payments industry and how the regulators had been responding to it around the world"[398]

[394]N.Y. City Bar Ass'n Formal Op. 2019-5 (2019).

[395] U.S. District Attorney's Office, Southern District of New York, "Former Law Firm Partner Sentenced To 10 Years In Prison For Laundering $400 Million of OneCoin Fraud Proceeds," (Jan. 25, 2024) https://www.justice.gov/usao-sdny/pr/former-law-firm-partner-sentenced-10-years-prison-laundering-400-million-onecoin-fraud.

[396] CORNELL LAW SCHOOL, https://support.law.cornell.edu/Students/forms/Concentration_Option.cfm, (last visited Feb. 15, 2024).

[397] CORNELL TECH, https://tech.cornell.edu/programs/masters-programs/master-of-laws-llm/, (last visited Feb. 16, 2024).

[398] MAURICE A. DEANE SCHOOL OF LAW AT HOFSTRA UNIVERSITY, https://bulletin.hofstra.edu/content.php?catoid=115&navoid=17317, (last visited Feb 15, 2024).

- *Pace* offers "Advanced Corporate Seminar: Regulation of Crypto," which "provides an overview of the various regulations that apply to the issuance and trading of cryptocurrency and other digital assets."[399]
- *Touro* offers "Fintech Law" which "explore[s] the impact of technology on legal issues in the financial services industry including topics such as regulatory issues in high-speed trading, the evolving use of block-chain technology in financial services, issues relating to cryptocurrency and non-fungible tokens (NFTs), initial coin offerings (ICO's), cybersecurity and data privacy issues, and the potential impact of artificial intelligence based systems on legal issues, such as property rights and tort liability."[400]

Law school clinics and centers educate students and the bar in this space as well:

- *Brooklyn Law's* Brooklyn Law Incubator & Policy Clinic ("BLIP") functions as a modern technology-oriented law firm where students are trained to represent emerging technology and Internet companies in addition to being at the "forefront of tech-related policy issues and advocate on behalf of causes and businesses in various legislative, regulatory, and judicial arenas."[401]
- *New York Law School's* Innovation Center for Law and Technology hosted "A Taste of Web3: Building Workshop," where participants learned how to build their own DAOs and websites that run on blockchain.[402]

New York law schools have had various publications and events related to crypto and DLT:

- *Brooklyn* has hosted a CLE called "Fintech and the Law: Power, Policy and Politics – Perspectives and Present Predictions on the Future of Crypto and Blockchain," which included a discussion on "pending legislative, regulatory, judicial, legal and policy issues governing blockchain, cryptocurrency, and other digital assets" and a keynote address from SEC Commissioner Jaime Lizárranga.[403] Brooklyn will also be hosting an event in April 2024 called "Reimagining the Future of FinTech Law and Policy," which will include a keynote and panel discussion with SEC Commissioner Hester M. Pierce.[404]
- *Cardozo's* Heyman Center on Corporate Governance held an event on "FTX and the Future of Crypto," which addressed "cryptocurrency exchanges, the issues

[399] ELISABETH HAUB SCHOOL OF LAW AT PACE UNIVERSITY, https://law.pace.edu/courses/advanced-corporate-seminar-regulation-crypto, (last visited Feb 15, 2024).
[400] TOURO UNIVERSITY JACOB D. FUCHSBERG LAW CENTER, https://www.tourolaw.edu/academics/coursedetails/668, (last visited Feb 15, 2024).
[401] BROOKLYN LAW SCHOOL, https://www.brooklaw.edu/Academics/Clinics%20and%20Externships/In-House%20Clinics/BLIP, (last visited Feb 15, 2024).
[402] NEW YORK LAW SCHOOL, https://www.nyls.edu/events/a-taste-of-web3-building-workshop/, (last visited Feb 15, 2024).
[403] BROOKLYN LAW SCHOOL, https://www.brooklaw.edu/News%20and%20Events/Events/2022/2022_11_16, (last visited Feb. 16, 2024).
[404] BROOKLYN LAW SCHOOL, https://www.brooklaw.edu/News-and-Events/Events/2024/2024_04_05, (last visited Feb. 16, 2024).

faced by FTX, why it collapsed, how bankruptcy will play out, and whether its executives face any legal liability."[405]

- *Columbia's* Blue Sky Blog has published various posts addressing emerging issues and developments in crypto "from academics, practitioners, industry professionals, and others."[406]
- *Touro* held a panel "Crypto is King," which addressed crypto law and job opportunities.[407]

Universities are already creating non-legal or legal adjacent courses and program offerings, showing an overall interest by students and universities in the topic:

- *Cornell's* SC Johnson College of Business offers an online course called "Trends in Fintech," which allows "participants analyze five major financial vertical markets in the fintech sector: robo-advising, peer-to-peer lending, insurance tech, currency and payment tech, and digital banking."[408]
- *Cornell's* SC Johnson College of Business also offers a two year MBA FinTech intensive, which "provides hands-on learning in the emerging financial technology sector."[409]
- *Fordham's* Gabelli School of Business offers a FinTech concentration.[410]
- *NYU* offers opportunities through its Emerging Technologies Collaborative, which is a cross-industry initiative designed to "lead in the convergence of the physical, digital, and virtual worlds impacting today's global industries, professions, [and] communities."[411] The collaborative hosts the podcast "Some Future Day," which "evaluates technology at the intersection of culture and law."[412] NYU Stern School of Business also offers a Master of Science in FinTech.[413]
- *St. John's* Peter J. Tobin College of Business offers a minor in Financial Technology (FinTech).[414]

---

[405] Heyman Center on Corporate Governance, "FTX and the Future of Crypto" (2022). *Event Invitations 2022*. 2. https://larc.cardozo.yu.edu/event-invitations-2022/2.

[406] COLUMBIA LAW SCHOOL, https://clsbluesky.law.columbia.edu/about-us/, (last visited Feb 15, 2024); *see also* COLUMBIA LAW SCHOOL, https://www.law.columbia.edu/search/content?keys=fintech+crypto#gsc.tab=0&gsc.q=fintech%20crypto&gsc.sort=, (last visited Feb 15, 2024).

[407] TOURO UNIVERSITY JACOB D. FUCHSBERG LAW CENTER, https://www.tourolaw.edu/AboutTouroLaw/Events/8561, (last visited Feb 15, 2024).

[408] CORNELL SC JOHNSON COLLEGE OF BUSINESS, https://ecornell.cornell.edu/courses/financial-management/trends-in-fintech/, (last visited Feb. 16, 2024).

[409] CORNELL SC JOHNSON COLLEGE OF BUSINESS, https://www.johnson.cornell.edu/programs/full-time-mba/two-year-mba/curriculum/intensives/fintech-intensive/, (last visited Feb. 16, 2024).

[410] FORDHAM GABELLI SCHOOL OF BUSINESS, https://bulletin.fordham.edu/gabelli-graduate/mba/concentrations/fintech/, (last visited Feb. 15, 2024).

[411] NEW YORK UNIVERSITY SCHOOL OF PROFESSIONAL STUDIES, https://www.sps.nyu.edu/homepage/emerging-technologies-collaborative.html, (last visited Feb. 15, 2024).

[412] NEW YORK UNIVERSITY SCHOOL OF PROFESSIONAL STUDIES, https://www.sps.nyu.edu/homepage/metaverse/metaverse-podcasts/some-future-day.html, (last visited Feb. 15, 2024).

[413] NEW YORK UNIVERSITY LEONARD N. STERN SCHOOL OF BUSINESS, https://www.stern.nyu.edu/programs-admissions/masters-programs/ms-fintech, (last visited Feb. 16, 2024).

[414] ST. JOHN'S UNIVERSITY PETER J. TOBIN COLLEGE OF BUSINESS, https://www.stjohns.edu/academics/programs/minor-financial-technology-fintech, (last visited Feb 15, 2024).

Article 7: Final Recommendations of the Report

Recommendation of the Task Force

A. *Create an Integrated Committee on Technology*:

This committee would combine the Task Force on Emerging Digital Finance & Currency, Committee on Law & Technology, and the Task Force on Artificial Intelligence and create a centralized group to continue to explore and study issues including but limited to:

- Continue to explore the way digital rights law interacts with Blockchain technology.
- Legal Adaptation and International Cooperation: The global nature of Web3 and blockchain transactions necessitates international legal cooperation to address copyright challenges. Developing standardized legal frameworks that recognize and enforce copyright across borders in the digital domain is essential for effective copyright protection in Web3.
- Legal Recognition of Digital Titles: Further study is needed to determine if laws should be enacted that recognize digital titles and registrations on a blockchain as legally valid and equivalent to traditional paper titles. This involves ensuring that digital records meet all legal requirements for real property transactions, including evidence of ownership, encumbrances, and liens. The idea of Implementing a hybrid system that maintains traditional title registration mechanisms while integrating blockchain technology should be evaluated as it may offer a transitional solution. This approach would leverage blockchain's efficiency and security while retaining the legal framework's established protections and recognitions.
- The question regarding the need for new Criminal Statutes to combat these new technologies remains open. This topic should continue to be explored. Illicit actors will always evolve along with the new technologies. These are new tools to accomplish existing crimes and similar outcomes. However, currently, there appears to be a sufficient number of statutes to enforce against the cases that are arising.
- IOLA Account Use by Attorneys: Attorneys are being presented with the opportunity to receive crypto funds for payment of services or to be held on behalf of clients. However, without crypto being recognized as a currency or bankable, it creates issues as to what mechanism they can use to hold these funds or even if the funds can be held as crypto to the fluctuating nature of the asset. Further study and analysis must be given to this issue.

- Currently, the USPTO and USCO have concluded that there is no need for changes to the trademark and copyright laws. However, this issue needs to continue to be studied. The unique nature of digital assets on blockchain platforms necessitates a rethinking of how trademark law is applied. For instance, the use of a specific digital asset (e.g., a unique piece of digital art or a character in a virtual world) as a brand identifier may require adaptations in trademark law to address issues of distinctiveness, use in commerce, and potential infringement in a decentralized context.

B. *Dispute Resolution and Enforcement:*

Developing new legal frameworks and dispute resolution mechanisms that can accommodate the decentralized nature of blockchain transactions is crucial. This might include specialized courts or arbitration panels familiar with blockchain technology and real property law.

C. *Use Emerging Technologies to Enhance Member Benefits:*

Initiate a request for proposals (RFP) from companies or organizations with expertise in emerging technology to integrate these technologies with those currently in use to increase member benefit and support.

ARTICLES 1, 2 & 3: Recommendations Regulatory Landscape

D. *Enact Clear Federal Legislation on Digital Assets:*

Congress should prioritize the enactment of clear, comprehensive federal legislation that specifically addresses the classification, taxation, and regulatory oversight of digital assets. This legislation should provide a definitive framework for determining when a digital asset is considered a security, commodity, or a new, distinct asset class. Additionally, the legislation should address the use of digital assets in various sectors, including finance, healthcare, and supply chain management.

E. *Improve and Enhance Appropriate Regulatory Frameworks and Oversight:*

To address the regulatory ambiguity and jurisdictional disputes, proposed legislation should aim to clearly define which agencies are responsible for regulating different aspects of the industry. This includes establishing more objective criteria for when and how crypto assets should move between regulatory regimes. By its nature, this is a global financial service. We need national oversight with state licensing like the rest of the financial and insurance industry.

<u>Regulatory bodies</u> should enhance its regulatory oversight of digital assets by:

- Developing a specialized division within the SEC dedicated to digital assets and blockchain technology. This division would be responsible for providing guidance, overseeing compliance, and enforcing regulations specific to digital assets.
- Collaborating with other regulatory agencies, such as the Commodity Futures Trading Commission (CFTC) and the Financial Crimes Enforcement Network (FinCEN), to ensure a coordinated and comprehensive regulatory approach.
- Review the applicability of the Howey Test and support statutory revisions to provide a clear framework.
- Creating a Clear Registration Scheme which would allow for Establishing counter parties, intermediaries, and exchanges.

F. *Establish a Regulatory Sandbox for Digital Assets:*

Regulatory sandboxes are innovative frameworks allowing businesses to test novel products and services in a controlled environment under regulatory supervision. This concept, drawing from the iterative testing approach commonly found in the tech industry, offers valuable insights for both regulators and innovators. It ensures that regulatory frameworks can adapt to technological advances while safeguarding consumer interests and maintaining financial stability.

The United States Federal and State Governments should create a regulatory sandbox that allows companies to develop and test innovative digital asset products and services within a safe harbor, under the guidance and supervision of regulators. The sandbox would offer a period of regulatory relief, during which companies can receive input from regulators on the development and alignment of their business models with legal and regulatory requirements.

G. *Foster Innovation and Collaboration:*

Advocate for regulatory bodies to foster innovation in the digital asset space by:

- Establishing appropriate regulatory sandboxes or pilot programs that allow for experimentation with digital asset technologies under a relaxed regulatory framework, subject to oversight and review.
- Promoting collaboration between regulators, academia, and the private sector to research and develop best practices for the use and regulation of digital assets.
- Supporting educational initiatives to enhance the understanding of digital assets and blockchain technology among regulators, law enforcement, and the general public.

H. *Taxation of Digital Assets and Currencies:*

The IRS has not provided taxpayers with sufficient opportunities to engage in discussions on the appropriate treatment of block rewards. As a result, there remains significant uncertainty around ancillary questions. We recommend that NYSBA

advocate for clear guidelines and rules regarding the taxation of digital assets and currencies.

Article 4: Intellectual Property Considerations in Web3

I. *International Cooperation and Harmonization:*

Given the global nature of Web3, there is a growing need for international cooperation and harmonization of trademark laws to tackle the challenges associated with branding digital assets. Developing standardized protocols for the registration, recognition, and enforcement of trademarks across borders could help mitigate some of the jurisdictional challenges posed by Web3.

J. Legal Recognition of Digital Titles:

Laws should recognize digital titles and registrations on a blockchain as legally valid and equivalent to traditional paper titles. This involves ensuring that digital records meet all legal requirements for real property transactions, including evidence of ownership, encumbrances, and liens.

Implementing a hybrid system that maintains traditional title registration mechanisms while integrating blockchain technology could offer a transitional solution. This approach would leverage blockchain's efficiency and security while retaining the legal framework's established protections and recognitions.

Article 5: Navigating the Nexus of Emerging Technologies and Criminal Justice: Challenges and Opportunities in the Age of Digital Currencies and Assets

K. *Continue to explore the implementation of the Use of Blockchain Technology in the Criminal Justice System to Enhance Efficiency and Access to Justice:*

Blockchain can be used to provide more secure access and more efficient storage and transfer of data such as for record keeping, maintaining police disciplinary data systems, service of process and to create uniform statewide pre-trial data collection. This will increase the integrity of the system and decrease wrongful convictions and unnecessary or prolonged incarceration.

L. *Consideration Should be Given to the Use of Digital Currency in Certain Aspects of the Criminal Justice System:*

Digital currencies are being used worldwide to bank the unbankable. Further, by their very nature, they provide a secure manner for the transfer of funds while

increasing accessibility. We recommend the use of Digital Currency be explored for bail, as a source of currencies for incarcerated people, restitution and for payment of fines and court fees.

M. *Importance of Cross Jurisdictional Cooperation & Collaboration:*

It is essential that the legal community continue to cooperate and develop cross-border relationships and collaborations to protect the communities and clients as well as provide the best opportunities for weeding out bad actors.

Article 6: Recommendations Ethics & Education

N. *Ethical Clarity Regarding Fee Arrangement Concerning Cryptocurrency:*

To avoid a potential ethical quagmire, when presented with a fee arrangement concerning cryptocurrency, the attorney should review the entire RPC, especially sections 1.5(a) and 1.8(a) to determine applicability and always act cautiously. Furthermore, whether RPC 1.8(a) could be reasonably implicated is immaterial, as any attorney holding cryptocurrency as a type of payment in advance should disclose the possible ethical issues implicated under RPC 1.8(a) in writing and further evaluate whether any other rules might be implicated. Being that an attorney is a fiduciary, the absence of such a writing, in the event there is an unexpected ethical quagmire, could result in an adverse inference regarding the attorney's conduct.

A way to avoid the pitfalls associated with an RPC 1.8(a) dilemma is to liquidate any cryptocurrency into fiat immediately upon receipt of payment. This is likely the more prudent approach to take, especially for an attorney not as familiar with cryptocurrency and until the tech is more universally adopted. Unless an attorney has the means necessary to adhere to the rules, better safe than sorry. Importantly, NYSBA should provide guidance as to whether attorneys can accept crypto as advanced payment for legal services.

O. *Continued Engagement in Law School Education:*

While law schools are increasingly doing their part to attempt to provide law students with opportunities to learn about these emerging technologies at the foundational level, the present bar must stay abreast of the changing technology. NYSBA should continue to engage with these programs.

P. *Best Practices:*

Develop best practices for attorneys engaging in the digital Assets & Crypto currency space. Attorneys must be diligent in following the guidelines of the

commentary to the Code of Ethics and ensure their actions do not violate any cannons or criminal laws. Attorneys must also be diligent in advising their clients on the importance of KYC to prevent unintended consequences.

Conclusion

Web3 represents a transformative shift toward decentralization and user empowerment, fundamentally propelled by blockchain technology. This new era challenges the centralized tenets of Web2, advocating for a digital realm where individuals exert unparalleled control over their data, identity, and assets. At the heart of this transformation is blockchain, which provides the critical infrastructure for secure, transparent, and intermediary-free interactions.

The migration to Web3 heralds significant implications for digital commerce and the management of data ownership, necessitating a redefinition of the legal and commercial frameworks that underpin digital engagements. In the Web3 environment, ownership of digital assets and personal data reverts to the individual, posing a direct challenge to the centralized data control and monetization models of established platforms.

Since the turn of the millennium, the ascent of digital currencies and the ecosystems supporting them have carved out new markets and forms of purchasing power. While these currencies have occasionally been co-opted for criminal activities, they also offer unprecedented opportunities for economic expansion, enhanced connectivity, and societal advancement.

For legal professionals, the rise of Web3 demands a thorough reevaluation of current legal norms to accommodate the decentralized, blockchain-based landscape. This includes grappling with complex issues such as jurisdiction, the enforceability of smart contracts, intellectual property rights in decentralized networks, and adherence to evolving data protection standards.

Additionally, the inherent decentralization of Web3 introduces novel challenges in governance, dispute resolution, and the application of traditional legal mechanisms within a dispersed digital framework. As legal practitioners, it is imperative that we explore how established legal principles adapt to a realm where transactions and interactions span a global, decentralized network devoid of centralized supervision.

This report aims to initiate a discussion on these pivotal issues, considering their implications for client representation, legislative and regulatory adaptation, and the integration of these emerging technologies within the practice of law and judicial processes. As we continue to navigate this uncharted territory, our understanding and responses must evolve to effectively address the unique challenges and opportunities presented by Web3.

The recommendations contained herein aim to establish policy of the New York State Bar Association consistent with its mission and to ensure that it remains the

leading voice of the New York legal community. With their adoption, the New York State Bar Associations (NYSBA) will be well positioned to be an integral part of shaping the future by being engaged in policy, regulatory and legislative developments.

Building upon the foundational shifts introduced by Web3, the New York State Bar Association plays a crucial role in continuously educating legal practitioners about these emerging technologies. As legal frameworks evolve in response to decentralization and blockchain technology, NYSBA is well-positioned to lead educational initiatives that ensure lawyers are proficient in this new legal landscape. This includes offering targeted training sessions, workshops, and CLE courses that address specific aspects of blockchain technology, digital currencies, and their implications for law practice.

Moreover, NYSBA has the opportunity to actively shape the discourse by taking well-informed positions on key issues affecting the legal community within the Web3 space. By advocating for sensible policies and regulations that protect user sovereignty while ensuring compliance and consumer protection, NYSBA can influence the development of laws that are both fair and forward-looking.

Recognizing that the transition to Web3 presents ongoing challenges and opportunities, NYSBA must establish a dedicated committee to address these issues specifically. This committee would monitor the evolving digital landscape, propose updates to legal practices as necessary, and serve as a bridge between technological innovators and the legal community. Its work would be critical in ensuring that legal practitioners remain at the forefront of technological advancements, ready to address new legal questions and advocate for regulatory approaches that protect both practitioners and the public.

Creating such a committee underscores the recognition that the work in adapting to Web3 is incomplete and will require sustained effort. As blockchain technology permeates various sectors, the legal implications will expand and deepen. A dedicated NYSBA committee would keep legal professionals informed and prepared and ensure they remain influential participants in shaping the future legal landscape around these transformative technologies.