Marquette Law Review

Volume 107
Issue 1 *Fall*

Article 5

2023

Blockchain Safe Harbor? Applying the Lessons Learned From Early Internet Regulation

Amy Cyphert

Sam Perl

Repository Citation

Amy Cyphert and Sam Perl, *Blockchain Safe Harbor? Applying the Lessons Learned From Early Internet Regulation*, 107 Marq. L. Rev. 145 (2023).
Available at: https://scholarship.law.marquette.edu/mulr/vol107/iss1/5

BLOCKCHAIN SAFE HARBOR? APPLYING THE LESSONS LEARNED FROM EARLY INTERNET REGULATION

AMY CYPHERT[*] & SAM PERL[**]

It has been more than a quarter century since Congress enacted twin safe harbor provisions to help protect and encourage the growth of a nascent internet by removing some liability and regulatory uncertainty. Today, there are calls for a similar safe harbor provision for blockchain, the technology behind cryptocurrencies and smart contracts. What lessons have we learned from the implementation of the internet safe harbor provisions, Section 230 of the Communications Decency Act, and Section 512 of the Digital Millennium Copyright Act? This Article charts the history of those provisions and their judicial construction over the decades. It also examines the criticism of these safe harbors, including that they have done too much to immunize large technology companies from the harm caused by their products. Blockchain technology shares a common history with the internet, and blockchain today is in a similar position to internet in the mid 1990s. Through cataloguing the lessons of internet regulation, this Article provides important considerations for regulators to bear in mind as they consider implementing safe harbor provisions for blockchain applications.

[*] Lecturer in Law & Director, ASPIRE Office, West Virginia University. This Article was supported, in part, by a Hodges Fund Faculty Research Grant. The authors are grateful to the following colleagues and friends for their feedback: Valarie Blake, Cody Corliss, Kirsha Trychta, and Elaine Wilson. The authors are also grateful to the staff of the *Marquette Law Review* for their careful and excellent work on this Article.

[**] Senior Member of the Technical Staff, CERT Division of the Software Engineering Institute, Carnegie Mellon University. Thank you to Robin Ruefle, the Security Operations Team, and the Monitoring and Response Directorate for their support.

I. INTRODUCTION

In February of 1996, from the rather unlikely location of Davos, Switzerland, a former Grateful Dead lyricist who had become a successful rancher in Wyoming declared the internet to be free of the "tyrannies" that the governments of the world would seek to impose upon it:

> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.
>
> . . . .
>
> Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is

> different.
>
> . . . .
>
> Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.[1]

John Perry Barlow was a songwriter and a rancher, but also a computer enthusiast who became the founder of the influential Electronic Frontier Foundation.[2] When he wrote his manifesto—A Declaration of the Independence of Cyberspace—the internet was at a critical inflection point. The early internet was inspired by "notions of anarchy and lawlessness."[3] "[E]arly [i]nternet was implemented at university computer science departments"[4] as well as by government researchers, and those creators "had little concern for controlling the network or its users' behaviors."[5] The design and code were "publicly available and freely shared."[6] But by 1996, the early days of the free internet—free to access, freely shared, free of laws—were waning and the internet had run solidly into the wall of regulation. Barlow's manifesto was written in response to passage of the Communications Decency Act, which would, among other things, attempt to address the issues of minors and obscene content on the internet.[7] Soon, the Digital Millennium Copyright Act would be passed, which criminalized the use of certain measures to circumvent technological restrictions on copying and accessing certain works.[8] The regulation of the internet had begun in earnest.

[1] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/8A5M-AEXF].

[2] John Perry Barlow's impact on the development of internet was so profound that the Duke Law and Technology Review hosted a special symposium in 2019 focused on him. James Boyle, *The Past and Future of the Internet: A Symposium for John Perry Barlow*, 18 DUKE L. & TECH. REV. 1, 1 (2019); *see also, e.g.*, Jonathan L. Zittrain, *John Perry Barlow's Call for Persuasion over Power*, 18 DUKE L. & TECH. REV. 137 (2019).

[3] PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 7 (2018).

[4] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 27 (2008).

[5] *Id.* at 28.

[6] *Id.*

[7] That specific provision—Title V—would later be struck down by the Supreme Court in *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) on First Amendment grounds.

[8] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 and 28 U.S.C.).

It has been roughly twenty-five years since the passage of the Communications Decency Act and the Digital Millennium Copyright Act. Each of those Acts included a safe harbor provision that was designed to help balance the need for internet regulation with an interest in fostering internet growth and innovation.[9] In the intervening twenty-five years, those safe harbor provisions have been construed by courts, lauded by supporters, and criticized by skeptics. They have also been applied to technology—such as social media—that was not even in existence at the time of their enactment. What have we learned about these safe harbor provisions and their impact in the roughly quarter century they have been around? This is not a mere rhetorical or academic question. Rather, it is a pressing one, because we are once again facing an inflection point with an emerging technology. Like early internet, this technology has emerged in part from the desire of its creators to escape centralized authorities, such as governments or banks, and to promote privacy and autonomy.[10] Further, this emerging technology has the potential to profoundly change the internet, ushering in an era of "web3."[11] Some scholars have even suggested that this technology "is as important as—or may even replace—the Internet."[12]

Blockchain technology is best known through its most famous (and infamous) application: cryptocurrencies like Bitcoin. But the technology is

[9] *See id.*; *see also* 47 U.S.C. § 230.

[10] *See, e.g.*, Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L.J. 487, 489 (2018) ("Proponents of blockchain technology describe it as a democratizing escape from the failings of territorial legal systems.").

[11] The term "Web3" refers to an internet built on tokens that are exchanged between developers and users, in lieu of credit card payments. *See, e.g.*, Kevin Roose, *What is web3?*, N.Y. TIMES (Mar. 20, 2022), https://www.nytimes.com/interactive/2022/03/18/technology/web3-definition-internet.html [https://perma.cc/GGW9-LUGS]. The term "Web 1.0" is used to refer to the early days of the world wide web (approximately 1985–2005), where adopters were posting websites that had less-dynamic features than today. "Web 2.0" (2005–today) is used to describe the explosion of dynamic web applications for services such as email, storage, mobile, and much more. "Web 3.0" is typically used to refer to the "Semantic Web," although this is still considered a work in progress. *See, e.g.*, Victoria Shannon, *A 'More Revolutionary' Web*, N.Y. TIMES (May 23, 2006), https://www.nytimes.com/2006/05/23/technology/23iht-web.html [https://perma.cc/542X-JQNW]. The origin of the term Web3 in a blockchain context is often traced to a blog post in 2014 by the Ethereum network co-founder Gavin Wood. He used the term Web 3.0 to describe internet services built upon decentralized blockchains. *See* Gavin Wood, *Less Techy: What is Web 3.0?*, GAVIN WOOD (Apr. 23, 2014) https://gavwood.com/web3lt.html [https://perma.cc/GJH7-4B29]. Other blockchain proponents adopted the term but changed it to Web3 so as to differentiate it from Web 3.0. *See* Chris Dixon, *Why Web3 Matters*, A16ZCRYPTO (Sept. 26, 2021), https://future.com/why-web3-matters/ [https://perma.cc/XBJ5-CR9S].

[12] DE FILIPPI & WRIGHT, *supra* note 3, at 46.

more than that one application, and includes applications like smart contracts that are growing in importance. The technology exists today much as early internet did in the mid-1990s, in a regulatory vacuum and grey area. But the recent calls for regulation of cryptocurrencies, calls spurred on by headlines dominated with high-profile cryptocurrency scandals, will no doubt change that.

What form should regulation of cryptocurrencies and other blockchain technologies take? Crucially, as lawmakers are increasingly called upon to regulate this technology and its applications, should blockchain applications receive a safe harbor provision? This Article proposes that we should consider the lessons learned from early internet regulation in answering these important and pressing questions. Part II examines the safe harbor provisions that were included in the Communications Decency Act and the Digital Millennium Copyright Act. Though those two safe harbor provisions include many similarities, they also include several key differences that have impacted the way they have been construed by courts. By charting judicial construction of those safe harbor provisions and examining the ways the provisions have been criticized and lauded over the years, certain patterns and best practices emerge, along with cautionary tales. Nearly all experts agree that Section 230 and Section 512 played an essential role in the development of the internet as we know it today. But at what cost?

Exploring the history of those sections makes clear that today's blockchain moment is not a new one. As Part III demonstrates, the cultural and philosophical movements that influenced early internet also influenced the early movement of cyberlibertarians known as "cypherpunks," a group of cryptographic enthusiasts who helped promote early blockchain technology. These original blockchain enthusiasts imagined a utopian ideal free of government censorship and regulation where people could privately and securely conduct their lives. The technology they developed was in service to those ideals. Of course, just as early internet "sought to decentralize power and encourage freedom of communication" but has nonetheless "become increasingly concentrated and regulated,"[13] so too has (and will) blockchain. Blockchain applications like cryptocurrencies and NFTs are dominant in today's news headlines. And yet, it can be difficult to understand what exactly a blockchain is. Thus, we trace the history of the technology, from early research papers to today's smart contracts. We also provide an overview of the technology in layman's terms.

[13] *Id.* at 7.

The heart of the Article is Part IV, where we examine certain safe harbor "best practices" for blockchain based on the lessons of early internet regulation. Blockchain regulation is likely imminent, and there is good reason to believe that regulation may include one or more safe harbor provisions; indeed, such safe harbor provisions have already been proposed in Congress and by a sitting SEC Commissioner. Further, safe harbor provisions are very common in not only internet regulation but also cybersecurity and other technology regulations. Thus, although we do not think advocates have yet made the case for a safe harbor for blockchain, especially for cryptocurrencies, and although we urge caution as regulators approach the topic, we also acknowledge that some form of safe harbor for blockchain may well be coming. Accordingly, we offer several important features that regulators should consider for an effective blockchain safe harbor. Safe harbors, when well designed, encourage desirable behavior and also provide some level of certainty that allows nascent technology to thrive. However, as the debate surrounding Section 230 demonstrates, a safe harbor that is too broad might incentivize (or even reward) undesirable behavior. Given the rapid pace of technological development, any safe harbor should include a sunset provision or at the very least be frequently revisited by Congress. We also discuss the need for a safe harbor provision to be clear and detailed to provide the kind of direction courts need. We address the need to balance industry involvement in the development of any blockchain safe harbor. Finally, we make the perhaps obvious but nonetheless important point that fraudulent behavior should not be given a safe harbor.

II. LESSONS LEARNED FROM THE HISTORY OF INTERNET REGULATION

When the internet first emerged, some legal scholars and commentators predicted that the internet would totally alter the existing systems of laws and governance. "No longer would the world be governed by nation-states, and no longer would governments be able to enact laws to establish fundamental rights, shape markets, or manage social interactions; rather, national laws and regulations would dissipate into the bits and bytes of 'cyberspace,' replaced by rules defined by private actors."[14] Of course, that's not what ultimately happened. Rather, governments around the world passed a variety of laws that govern internet service providers, that regulate how internet can be accessed, and that dictate the ways in which traditional regulation applies to cyber

[14] *Id.* at 50. De Filippi and Wright cite scholars who advanced this argument, but note that "these early prognostications about the unregulatability of the Internet were found to be overly broad." *Id.*

applications. Two of the most important laws were passed in the United States within two years of each other. The Communications Decency Act and the Digital Millennium Copyright Act have much in common, including that both were an attempt to offer some protection to the burgeoning internet industry (and, indeed, many commentators argue today's internet would not exist without both of these Acts).[15] And yet, they also include important differences, especially in their safe harbor provisions, and courts have accordingly construed them at times in different ways.

A. Section 230 of the Communications Decency Act

i. History of Section 230

In the early 1990s, online service providers like Prodigy, CompuServe, and AOL had a problem. The companies were facing large-scale legal liability from defamation lawsuits brought because of the content that others posted to the forums, bulletin boards, and chat rooms that the companies provided online access to.[16] The judges assigned to these cases also had a problem: were these companies *publishers* of content, like newspapers? Or were they *distributors* of content, like newsstands or bookstores? Much liability hung on the answer to that question, since publishers were strictly liable for republishing a defamatory statement[17] while distributors were only liable if they knew or should have known that the statement was defamatory.[18]

New York courts would lead the way in determining whether online service providers were publishers or distributors. The first court to reach the question

[15] *See* Lenz v. Universal Music Corp., 815 F.3d 1145, 1149–50 (9th Cir. 2016).

[16] *See, e.g.*, Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 135 (S.D.N.Y. 1991) (discussing claim of defamation against CompuServe for content posted to its forums); Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710, at *1 (N.Y. Sup. Ct. May 24, 1995) (discussing claim of defamation against Prodigy for content posted by a user to its bulletin board).

[17] *See, e.g.*, Cianci v. New Times Publ'g Co., 639 F.2d 54, 61 (2d Cir. 1980); *see also Prodigy Servs. Co.*, 1995 WL 323710, at *3 (citations omitted) (citing Mia. Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 258 (1974)) ("[A] newspaper . . . is more than a passive receptacle or conduit for news, comment and advertising. The choice of material to go into a newspaper and the decisions made as to the content of the paper constitute the exercise of editorial control and judgment, and with this editorial control comes increased liability."); RESTATEMENT (SECOND) OF TORTS § 578 (AM. L. INST. 1977) ("[O]ne who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it.").

[18] *See, e.g.*, *Cubby, Inc.*, 776 F. Supp. at 139 (citing Smith v. California, 361 U.S. 147, 152–53 (1959)) ("The requirement that a distributor must have knowledge of the contents of a publication before liability can be imposed for distributing that publication is deeply rooted in the First Amendment, made applicable to the states through the Fourteenth Amendment.").

was a federal court in Manhattan that ruled in 1991 that CompuServe was a news distributor, not a publisher.[19] At the time, CompuServe offered subscribers access to "over 150 special interest 'forums,' which [were] comprised of electronic bulletin boards, interactive online conferences, and topical databases."[20] The case arose from allegedly defamatory statements published to one of the journalism forums (involving the apparently aptly named parties "Rumorville" and "Skuttlebut").[21] The court held that because CompuServe had no "editorial control" over the content posted to the site, it was more akin to a public library than a newspaper, and so was a distributor, not a publisher.[22] The court further held that CompuServe was not liable as a distributor for allegedly defamatory statements that subscribers could access on its service, as there was no evidence in the record that the company knew or should have known about the statements.[23]

Four years later, a New York state court judge, while claiming to be "in full agreement" with the *Cubby v. CompuServe* decision, took a different view.[24] The court in *Stratton Oakmont, Inc. v. Prodigy Services Co.* examined whether Prodigy could be held liable for allegedly defamatory comments posted to one of its bulletin boards.[25] In granting partial summary judgment, the court held that Prodigy was a publisher, and was thus held to the heightened liability standard in a defamation case.[26] Ironically, one rationale the court offered for holding Prodigy to the higher standard was the company's own attempts at content moderation through practices such as the "use of a software screening program which automatically prescreen[ed] all bulletin board postings for offensive language."[27] The judge noted that Prodigy had "held itself out as an

[19] *Id.* at 135.

[20] *Id.* at 137.

[21] *Id.* at 137–38.

[22] *Id.* at 140 (noting that when CompuServe "decide[s] to carry a publication, it will have little or no editorial control over that publication's contents").

[23] *Id.* ("CompuServe has no more editorial control over such a publication than does a public library, book store, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so.").

[24] Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710, at *5 (N.Y. Sup. Ct. May 24, 1995).

[25] *Id.*

[26] *Id.* at *4.

[27] *Id.* at *2; *see also* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET 38 (2019) (noting that CompuServe and Prodigy took different approaches to reviewing content before

online service that exercised editorial control over the content of messages posted on its computer bulletin boards, thereby expressly differentiating itself from its competition and expressly likening itself to a newspaper."[28] The *Prodigy* decision set in motion a bipartisan effort that would change the future of the internet.

Representative Chris Cox, flying back to Washington, D.C. from his home in California, read an article about the *Prodigy* decision and thought it made little sense that Prodigy would be held to a heightened liability standard because it attempted to do some content moderation, while CompuServe would be spared because it did not.[29] Unlike many of his congressional colleagues at the time, Representative Cox used both CompuServe and Prodigy and saw the chilling effect these defamation lawsuits would have on the industry.[30] He reached out to Representative Ron Wyden, a Democrat from Oregon, and the two talked about how to properly incentivize technology companies to moderate online content.[31] The two sought a bipartisan approach that would avoid smothering the nascent industry with overregulation but would also avoid the ironic outcome of the *Prodigy* decision wherein companies could avoid liability by doing no content moderation.[32] The duo thought that "empower[ing] Internet companies—and their subscribers—to figure out the rules that govern their communities" was the right approach.[33] As Representative Cox would later reflect, "[w]hat we were trying to do was to make sure the people who were in the best position to clean up the Internet would do so."[34]

Cox and Wyden worked quickly, and were joined in their work by a lawyer from America Online and a lawyer from Prodigy, meeting often to draft legislation.[35] A mere five weeks after the *Prodigy* decision was issued, they proposed the bill that would ultimately come to be known as Section 230 of the Communications Decency Act of 1996.[36] As one of us has argued previously, the legislative history of Section 230 makes "clear that Congress had an

providing it to their subscribers, with CompuServe adopting a more hands-off approach and Prodigy "creat[ing] and enforc[ing] user conduct standards").

[28] *Prodigy Servs. Co.*, 1995 WL 323710, at *2.

[29] KOSSEFF, *supra* note 27, at 59.

[30] *Id.*

[31] *Id.* at 59–60.

[32] *Id.* at 60.

[33] *Id.*

[34] *Id.* (citing the author's April 14, 2017, interview with Chris Cox).

[35] *Id.* at 61.

[36] *Id.* at 64.

optimistic view of the future of discourse on the internet" at the time of its passage.[37] Section 230 provides that no user or provider of an "interactive computer service" shall be treated as "the publisher or speaker" of information that was provided by another "content provider."[38] This key language is found in (c)(1) of the Section, and has been called the "twenty-six words that created the internet."[39]

ii. Judicial Construction of Section 230

Courts have consistently construed Section 230 broadly. The first courts to look at the language immediately confirmed that companies like Prodigy and CompuServe were providers of "interactive computer services."[40] One year after Section 230 was passed, the Fourth Circuit confirmed that AOL was also an interactive computer service.[41] Courts have since found that social media companies, dating apps, and online shopping sites are all interactive computer services that are entitled to Section 230 protection.[42] As the Ninth Circuit has

[37] Amy B. Cyphert & Jena T. Martin, *"A Change is Gonna Come:" Developing a Liability Framework for Social Media Algorithmic Amplification*, 13 U.C. IRVINE L. REV. 155, 172 (2022) (footnote omitted) (quoting 47 U.S.C. § 230(a)(1)–(3)) ("The findings that begin the Section describe the internet as 'an extraordinary advance in the availability of educational and informational resources to our citizens,' and as something that offers 'a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.'").

[38] 47 U.S.C. § 230(c)(1).

[39] KOSSEFF, *supra* note 27. Kosseff titled his book "The Twenty-Six Words That Created the Internet" and describes Section 230 therein as the twenty-six words that "have created the modern Internet." *Id.* at 2. The full text of 47 U.S.C. § 230(c)(1) is: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

[40] The definitional portion of Section 230 defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(f)(2).

[41] Zeran v. Am. Online, Inc., 129 F.3d 327, 329 (4th Cir. 1997).

[42] Cyphert & Martin, *supra* note 37, at 173 ("Courts have continued to define the term broadly in the years since, with cases declaring Grindr, Twitter, MySpace, and Amazon all to be interactive computer services under Section 230.").

noted, the most common interactive computer services under Section 230 are websites,[43] and courts construe the definition broadly.[44]

Courts have also construed the term "content provider" in the years since Section 230's passage.[45] Several circuits have adopted variations of what is known as the "material contribution" test to determine whether a website is a content provider or merely a forum for the content of a third party.[46] The Ninth Circuit has held that "a website that 'creat[es] or develop[s]' content 'by making a material contribution to [its] creation or development' loses [Section] 230 immunity."[47] As that court has noted, "'material contribution' does not refer to 'merely . . . augmenting the content generally, but to materially contributing to its alleged unlawfulness.'"[48]

Courts have so narrowly defined content provider that they have even held that Section 230 immunizes websites from the affirmative actions they take, often algorithmically, to promote and recommend the content of others through recommendation systems. The Second Circuit, for example, held that "[m]erely arranging and displaying others' content to users of Facebook through [recommendation] algorithms—even if the content is not actively sought by those users—is not enough to hold Facebook responsible as the 'develop[er]'

[43] *See* Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008) ("Today, the most common interactive computer services are websites.").

[44] *See* Kimzey v. Yelp! Inc., 836 F.3d 1263, 1268 (9th Cir. 2016) (quoting Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003)) (noting that the term "interactive computer service" is "interpret[ed] 'expansively' under the CDA").

[45] The definitional portion of Section 230 defines "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(f)(3).

[46] *See*, *e.g.*, Gonzalez v. Google LLC, 2 F.4th 871, 892 (9th Cir. 2021), *cert. granted sub nom.* Twitter, Inc. v. Taamneh, 143 S. Ct. 81 (2022) (mem.); F.T.C. v. LeadClick Media LLC, 838 F.3d 158, 176 (2d Cir. 2016) (alteration in original) (quoting *Roommates.Com*, 521 F.3d at 1168) (denying Section 230 immunity where the defendant "participated in the development of its affiliates' deceptive websites, 'materially contributing to [the content's] alleged unlawfulness'"); Jones v. Dirty World Ent. Recordings LLC, 755 F.3d 398, 413 (6th Cir. 2014) (alteration in original) (quoting 47 U.S.C. § 230(f)(3)) ("Consistent with our sister circuits, we adopt the material contribution test to determine whether a website operator is 'responsible, in whole or in part, for the creation or development of [allegedly tortious] information.'"); F.T.C. v. Accusearch Inc., 570 F.3d 1187, 1199 (10th Cir. 2009) ("We therefore conclude that a service provider is 'responsible' for the development of offensive content only if it in some way specifically encourages development of what is offensive about the content.").

[47] *Gonzalez*, 2 F.4th at 892 (citing *Kimzey*, 836 F.3d at 1269).

[48] *Id.* (quoting *Roommates.Com*, 521 F.3d at 1167–68) (emphasis added).

or 'creat[or]' of that content."[49] This is true even when plaintiffs allege that a company's recommendation algorithms allowed groups like Hamas to more easily recruit members.[50] The Ninth Circuit has similarly held that YouTube's recommendation algorithms do not render it a content provider under Section 230, even if those algorithms allegedly recommend that viewers watch violent propaganda from ISIS.[51] As noted above, Section 230 was drafted in part to protect websites from liability for the decision to remove harmful content. But courts today extend it to decisions to promote harmful content as well.

iii. Criticism of Section 230

Even as courts have consistently construed Section 230's protections broadly and have repeatedly found that they immunize websites for the content of others and the website's own decisions to promote that content, there have been dissenters. Indeed, one dissenting judge in the Ninth Circuit noted that "there is a rising chorus of judicial voices cautioning against an overbroad reading of the scope of Section 230 immunity."[52] Further, there is some indication that Congress may act, given the bipartisan support for reforming Section 230.[53] Many academics have joined judges who are skeptical about the breadth of the immunity as well and have joined calls for reform.[54]

We will need to wait on guidance from the Supreme Court on this issue. On October 3, 2022, the Court granted certiorari in *Gonzalez v. Google* on the question, "Does section 230(c)(1) immunize interactive computer services

[49] Force v. Facebook, Inc., 934 F.3d 53, 70 (2d Cir. 2019).

[50] *Id.*; *see also* Marshall's Locksmith Serv. Inc. v. Google, LLC, 925 F.3d 1263, 1271 (holding that "automated editorial act[s]" are protected by Section 230).

[51] *Gonzalez*, 2 F.4th at 913.

[52] *Id.* at 896. The majority, although holding that Section 230 immunity applied in the case, nonetheless noted: "We share the dissent's concerns about the breadth of § 230." *Id.*

[53] *See* Cyphert & Martin, *supra* note 37, at 168–69 (discussing bipartisan support for reforming Section 230); *see also Gonzalez*, 2 F.4th at 897 ("In light of the demonstrated ability to detect and isolate at least some dangerous content, Congress may well decide that more regulation [regarding § 230] is needed.").

[54] *See, e.g.*, Olivier Sylvain, *Platform Realism, Informational Inequality, and Section 230 Reform*, 131 YALE L.J. F. 475, 477 (2021) ("Reform [of Section 230] is urgently needed because online service designs produce outcomes that conflict with hard-fought but settled consumer-protection and civil-rights laws."); Lauren Rundall, *Don't Break the Internet: § 230 and Its Role Within Today's Modern Internet Era*, 5 BUS. ENTREPRENEURSHIP & TAX L. REV. 50, 63–64 (2021) ("Section 230 is crucial in order to maintain an open and free internet space, but some changes need to be made to reflect the internet's role today and to prevent massive social media companies from exerting too much power and having too large an influence in what content users consume.").

when they make targeted recommendations of information provided by another information content provider, or only limit the liability of interactive computer services when they engage in traditional editorial functions (such as deciding whether to display or withdraw) with regard to such information?"[55] Many commentators believed the Court would potentially upend years of jurisprudence on the scope of Section 230.[56] However, the Court did not reach the substantive issue, choosing instead to send the case back to the Ninth Circuit "without ruling on the parameters of Section 230."[57]

B. Section 512 of the Digital Millennium Copyright Act

i. History of Section 512

Section 230 was not the only safe harbor provision that Congress saw fit to implement in the late 1990s to address emerging problems on the internet. In 1998, Congress passed the Digital Millennium Copyright Act (DMCA). The DMCA brought U.S. copyright law into compliance with two World Intellectual Property Organization treaties that the U.S. was a signatory to that addressed copyright issues for the digital age.[58] The DMCA was "designed to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age."[59] The Act both extended the reach of copyright laws, updating

[55] Question Presented Report, Gonzalez v. Google LLC, 598 U.S. 617 (2023) (No. 21-1333), https://www.supremecourt.gov/qp/21-01333qp.pdf [https://perma.cc/HW9G-UCYP].

[56] *See, e.g.*, Scott R. Anderson, Quinta Jurecic, Alan Z. Rozenshtein & Benjamin Wittes, *The Supreme Court Punts on Section 230,* LAWFARE BLOG (May 19, 2023, 12:00 PM), https://www.lawfaremedia.org/article/the-supreme-court-punts-on-section-230 [https://perma.cc/5PHA-SW9J] ("The Supreme Court's big case on Section 230, Gonzalez v. Google, was going to rewrite the law of electronic communications.").

[57] *Id.*

[58] MDY Indus., LLC v. Blizzard Ent., Inc., 629 F.3d 928, 942 (9th Cir. 2010), *amended and superseded on denial of reh'g*, No. 09-15932, 2011 WL 538748 (9th Cir. Feb. 17, 2011) ("Congress enacted the DMCA in 1998 to conform United States copyright law to its obligations under two World Intellectual Property Organization ("WIPO") treaties, which require contracting parties to provide effective legal remedies against the circumvention of protective technological measures used by copyright owners."); *see also* Laura A. Possessky, *Throwing the Baby Out with the Bathwater*: Lenz v. Universal *and the Future of DMCA Safe Harbor Takedown Notifications*, 8 LANDSLIDE 10, 11 (2016) (footnote omitted) (noting that in passing the DMCA, Congress "grappled with the task of adopting legislation to implement World Intellectual Property Organization (WIPO) treaties, which required signatory countries to provide greater copyright protection through anticircumvention and preventing tampering with copyright management information").

[59] S. REP. NO. 105-190, at 1–2 (1998).

them for the internet age, while also simultaneously limiting the liability of online service providers for any infringing material posted by their users.[60]

Just as the concerns online service providers had about defamation liability spurred Congress to pass Section 230, so too the concerns that these providers had about liability for copyright infringement helped spur the DMCA, as these were concerns that Congress was "sympathetic to."[61] The Act included a safe harbor provision that was designed to ease the fears service providers had about liability for copyright infringement.[62] The resulting legislation—Section 512—provided a safe harbor for service providers who hosted "infringing user content."[63] To be eligible for the safe harbor, service providers were required to "adopt and implement a policy for terminating repeat infringing subscribers" and "accommodate and refrain from interfering with standard technical measures used by copyright owners to identify or protect copyrighted works."[64]

Section 512(c) provided the basic contours of the safe harbor provision for service providers who host infringing content.[65] In order to be eligible, a service provider had to not have actual knowledge that it was hosting copyrighted information, and, if it was made aware that it was hosting copyrighted information, had to "act[] expeditiously to remove, or disable access to, the material."[66] Thus, Section 512(c) required that service providers who received

[60] *See MDY Indus., LLC*, 629 F.3d at 942 ("In enacting the DMCA, Congress sought to mitigate the problems presented by copyright enforcement in the digital age.").

[61] S. REP. NO. 105-190, at 19 n.20 (1998) ("Although the copyright infringement liability of on-line and Internet service providers (OSPs and ISPs) is not expressly addressed in the actual provisions of the WIPO treaties, the Committee is sympathetic to the desire of such service providers to see the law clarified in this area.").

[62] *Id.* ("There have been several cases relevant to service provider liability for copyright infringement. Most have approached the issue from the standpoint of contributory and vicarious liability. Rather than embarking upon a wholesale clarification of these doctrines, the Committee decided to leave current law in its evolving state and, instead, to create a series of 'safe harbors,' for certain common activities of service providers. A service provider which qualifies for a safe harbor, receives the benefit of limited liability.").

[63] Greg Jansen, *Whose Burden Is It Anyway? Addressing the Needs of Content Owners in DMCA Safe Harbors*, 62 FED. COMM. L.J. 153, 161 (2010).

[64] *Id.* at 161–162; *see also* 17 U.S.C. § 512(i)(1)–(i)(2).

[65] The DMCA also contains safe harbor provisions for service providers who operate systems that others use to transmit infringing material through 17 U.S.C. § 512(a); for service providers who temporarily store infringing material ("caching") through 17 U.S.C. § 512(b); and for service providers who "refer[] or link[] users to an online location containing infringing material or infringing activity" through 17 U.S.C. § 512(d). Although, 17 U.S.C. § 512(c) is the safe harbor provision most akin to Section 230, and is thus the safe harbor provision this Article focuses most heavily on.

[66] 17 U.S.C. § 512(c)(1)(A)(iii).

a notification from a copyright holder that the provider was hosting copyrighted material promptly take down the offending material.[67] These Section 512(c) compliance procedures have come over the years to be known as the DMCA's "takedown procedures."[68]

Section 512(c)(3)(A) outlined in detail the content that a copyright holder should include when contacting a service provider to request the removal of their copyrighted material. The copyright holder had to include a statement that they had "a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law," and that "the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed."[69] Service providers developed systems wherein copyright holders could notify them that they were hosting an allegedly infringing work. These often took the form of automated webforms.[70]

In order to protect users from false claims that they were posting copyrighted material, Section 512 of the DMCA required that any time a service provider receive a takedown notice, it had to promptly notify the user who had posted the allegedly copyrighted material.[71] "The user then has the option of restoring the content by sending a counter-notification, which must include a statement of 'good faith belief that the material was removed or disabled as a result of mistake or misidentification.'"[72] If the provider receives a valid counter-notification, it has to restore access to the material within ten to fourteen days (unless it receives notice that the copyright holder was suing the

[67] *See id.* § 512(c); *see also* Lenz v. Universal Music Corp., 815 F.3d 1145, 1151 (9th Cir. 2016) ("Section 512(c) permits service providers, e.g., YouTube or Google, to avoid copyright infringement liability for storing users' content if—among other requirements—the service provider 'expeditiously' removes or disables access to the content after receiving notification from a copyright holder that the content is infringing.").

[68] *Lenz*, 815 F.3d at 1151 ("The procedures outlined in § 512(c) are referred to as the DMCA's 'takedown procedures.'").

[69] 17 U.S.C. § 512(c)(3)(A)(v)–(vi).

[70] Peter Cramer & David Munkittrick, *Will NFT Piracy Compel Changes to the Digital Millennium Copyright Act?*, PROSKAUER (Mar. 16, 2022), https://www.blockchainandthelaw.com/2022/03/will-nft-piracy-compel-changes-to-the-digital-millennium-copyright-act/ [https://perma.cc/TH6W-LT8X] ("[M]ost online service providers introduced 'Notice-and-Takedown' systems, usually automated webforms, through which copyright owners could flag infringing user posts for removal.").

[71] 17 U.S.C. § 512(g)(1)–(2).

[72] *Lenz*, 815 F.3d at 1151 (quoting 17 U.S.C. § 512(g)(3)(c)).

user for copyright infringement).[73] The requirements laid out in Section 512(g) have come to be known as the DMCA's "put-back procedures."[74]

ii. Judicial Construction of Section 512

Courts have had many opportunities to construe the DMCA's safe harbor provisions in the twenty-five years since its passage.[75] In much the same way that courts were left to apply Section 230 to a changed technological landscape (by, for example, applying it to social media company algorithmic amplification, a concept and entire industry that did not exist at the time of the law's passage), so too have courts had to apply the DMCA to technologies that did not exist at the time of the law's passage in 1998. For example, some scholars have noted that courts have struggled to apply the DMCA's safe harbor protections to peer-to-peer networking and file sharing technologies.[76] As technology continues to evolve, the DMCA safe harbor provisions may become increasingly less meaningful.[77] For example, the DMCA takedown provisions

[73] 17 U.S.C. § 512(g)(2)(c) (limiting liability for a service provider who "replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network").

[74] *Lenz*, 815 F.3d at 1151 ("The procedures outlined in § 512(g) are referred to as the DMCA's 'put-back procedures.'").

[75] Interestingly, the copyright safe harbor concept was a judicial construction before it was codified by Congress in the DMCA. *See* Tonya M. Evans, *"Safe Harbor" for the Innocent Infringer in the Digital Age*, 50 WILLAMETTE L. REV. 1, 26 (2013) (citing Sony v. Universal City Studios, 464 U.S. 417 (1984)) ("In the Sony Betamax case, the Supreme Court articulated the first safe harbor, a creature of judicial construction that predates the DMCA.").

[76] *See, e.g.*, Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 113 (2007) (noting that the DMCA's safe harbor provisions "were drafted in 1998 to carve out specific intermediaries, rather than creating a general protection for Internet intermediaries hosting, passing through, or linking to the content of another. As a result, they almost immediately became obsolete as new technologies – most notably p2p networking – were developed").

[77] *See id.* ("As new business models develop, and as companies in the existing categories change the way they work, the specific categories of the DMCA are likely to be less and less relevant.").

are arguably less effective against blockchain-based applications like NFTs,[78] discussed in greater detail below.[79]

Further, courts have had to engage in gap-filling exercises to decide cases that turned upon ambiguous or undefined terms in the DMCA,[80] despite the fact that the DMCA was enacted in part to avoid a flood of lawsuits.[81] Just as courts did when construing Section 230, courts construing the DMCA safe harbor provisions have tended to construe them broadly. For example, courts have concluded that the DMCA protects service providers from both direct copyright infringement, as well as contributory infringement.[82] In the 2001 case *A&M Records, Inc. v. Napster, Inc.*, record companies brought a copyright infringement suit against Napster, which facilitated the peer-to-peer sharing of MP3 music files amongst its users.[83] Citing the legislative history of the DMCA, the Ninth Circuit rejected the district court's determination that the Act's safe harbor provisions did not provide protection to service providers for contributory infringement.[84]

[78] *See, e.g.*, Rebecca Carroll, *NFTs: The Latest Technology Challenging Copyright Law's Relevance Within a Decentralized System*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 979, 1000 (2022) (addressing the applicability of the DMCA to NFTs and noting that "[w]hile blockchain technology can be used to trace secondary transactions of an infringing NFT from the seller to each subsequent buyer, those parties likely transact under a pseudonym, making it nearly impossible for an artist to bring a viable claim against infringers," and also mentioning that "with the volume of marketplaces and the seller's ability to list the same infringing artwork as an NFT across a number of venues, it is much more difficult for an artist to discover all infringing uses before the work is sold").

[79] *See infra* Section III.C.

[80] *See, e.g.*, Jessica Di Palma, *The Digital Millennium Copyright Act and the Clash Between Authors and Innovators: The Need for A Legislative Amendment to the Safe Harbor Provisions*, 47 LOY. L.A. L. REV. 797, 800 (2014) ("Congress failed to adequately define the requirements an ISP must meet to fall within a safe harbor provision, which has left the door open for courts to tailor these requirements appropriately to meet the needs of evolving technologies.").

[81] *See id.* at 805 ("While Congress intended the safe harbor provisions under § 512(c) to resolve potential digital copyright suits without the courts' help, § 512(c) has instead opened the floodgates to litigants disputing exactly how the safe harbor protections should be interpreted."); *see also* Lital Helman & Gideon Parchomovsky, *The Best Available Technology Standard*, 111 COLUM. L. REV. 1194, 1205 (2011) ("One of Congress's goals in enacting the section 512(c) safe harbor was to increase legal certainty for webhosts. Yet section 512(c) as it currently stands falls short of this mark.").

[82] "Contributory liability requires that the secondary infringer 'know or have reason to know' of direct infringement." A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1020 (9th Cir. 2001), *aff'd*, A&M Recs., Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002).

[83] *Napster, Inc.*, 284 F.3d at 1093.

[84] *See id.* at 1025 ("We need not accept a blanket conclusion that § 512 of the Digital Millennium Copyright Act will never protect secondary infringers."). The *Napster* case is especially

As with Section 230, courts that have construed the DMCA safe harbor provisions have often read them in favor of service providers.[85] For example, courts have held that the DMCA does not generally require that service providers actively police for infringing content to be eligible for the Section 512 safe harbor.[86] Although this much is arguably clear from the plain text of the statute,[87] courts have extended this and held that because the DMCA does not require affirmative policing of copyright, it also limits the ability of plaintiffs to claim a company was "willfully blind" to copyright infringement.[88] In *Viacom International, Inc. v. YouTube, Inc.*, the plaintiffs (which included film studios, television networks, music publishers, and sports leagues) filed suit against YouTube and other defendants alleging direct and secondary copyright infringement for clips that appeared on that website.[89] The district court granted summary judgment, holding that YouTube was entitled to DMCA safe harbor protection.[90] Plaintiffs argued that the defendants were not entitled to the safe harbor protection because, among other reasons, "YouTube was 'willfully blind' to specific infringing activity."[91] In upholding that portion of the district court opinion, the Second Circuit held that, despite the fact that the

relevant when thinking about blockchain, since Napster's model relied on a peer-to-peer system for filesharing. The courts ultimately ordered Napster to shut down its filesharing service, after concluding that a preliminary injunction was not enough to stop the sharing of copyrighted materials. *See id.* at 1096 ("After three months of monitoring, the district court determined that Napster was not in satisfactory compliance with the modified preliminary injunction. The district court ordered Napster to disable its file transferring service until certain conditions were met and steps were taken to ensure maximum compliance."). The company ultimately filed for bankruptcy. Andrew Dansby, *Napster Files for Bankruptcy*, ROLLING STONE (June 4, 2002), https://www.rollingstone.com/music/music-news/napster-files-for-bankruptcy-246468/ [https://perma.cc/WZM8-LAUD].

[85] *See, e.g.*, Disney Enters., Inc. v. Hotfile Corp., No. 11-20427-CIV, 2013 WL 6336286, at *19 (S.D. Fla. Sept. 20, 2013) ("Although an affirmative defense, the DMCA has often been construed in favor of service providers, requiring relatively little effort by their operations to maintain immunity.").

[86] *See, e.g.*, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 35 (2d Cir. 2012) ("Section 512(m) is explicit: DMCA safe harbor protection cannot be conditioned on affirmative monitoring by a service provider.").

[87] 17 U.S.C. § 512(m)(1) (noting that the safe harbor protections are not contingent upon "a service provider monitoring its service or affirmatively seeking facts indicating infringing activity"); *see also* Capitol Recs., LLC v. Vimeo, LLC, 826 F.3d 78, 98 (2d Cir. 2016) ("Protecting service providers from the expense of monitoring [for infringing content] was an important part of the compromise embodied in the safe harbor.").

[88] *Viacom Int'l*, 676 F.3d at 35.

[89] *Id.* at 25–26.

[90] *Id.* at 26.

[91] *Id.* at 34.

words "willful blindness" are nowhere in the DMCA,[92] the safe harbor provisions in Section 512 nonetheless limit that doctrine.[93]

However, as they construe Section 512 claims, courts have also tried to balance the rights of users who post allegedly infringing content.[94] In *Lenz v. Universal Music Corp.*, the Ninth Circuit made clear that copyright holders who believe their work is being infringed upon "must consider the existence of fair use before sending a takedown notification under [the DMCA]."[95] In other words, a copyright owner should not file a DMCA takedown notice without first examining whether the use they object to might fall into a copyright exception such as fair use. In *Lenz*, a mother had made a twenty-nine second video of her two children in their kitchen, dancing to Prince's song *Let's Go Crazy*, and posted it to YouTube.[96] Universal, who "was Prince's publishing administrator responsible for enforcing his copyrights," filed a takedown notice with YouTube, which removed Lenz's video.[97] Lenz brought suit, arguing that Universal was required to consider whether her video was fair use prior to sending the takedown notice.[98] The Ninth Circuit ultimately agreed, holding that "the DMCA requires consideration of fair use prior to sending a takedown notification" and that a jury should hear the case.[99]

iii. Criticisms of Section 512

Section 512 has been lauded in much the same way as Section 230 and deemed crucial to the development of the internet as we know it.[100] But, just

[92] *Id.* at 35 ("The DMCA does not mention willful blindness.").

[93] *Id.*

[94] The 2020 U.S. Copyright Office Report on Section 512 noted that there have been recent court decisions "more favorable to copyright owners." U.S. COPYRIGHT OFF., SECTION 512 OF TITLE 17: A REPORT OF THE REGISTER OF COPYRIGHTS 97 (2020), https://www.copyright.gov/policy/section512/section-512-full-report.pdf [https://perma.cc/JW9K-TQ7G] (citing BMG Rights Mgmt. LLC v. Cox Commc'ns, Inc., 881 F.3d 293 (4th Cir. 2018); UMG Recordings, Inc. v. Grande Commc'ns Networks, Inc., 384 F. Supp. 3d 743 (W.D. Tex. 2019)).

[95] Lenz v. Universal Music Corp., 815 F.3d 1145, 1153 (9th Cir. 2016).

[96] *Id.* at 1149.

[97] *Id.* at 1149–50.

[98] *Id.* at 1148.

[99] *Id.* at 1154.

[100] *See* KOSSEFF, *supra* note 27, at 121 (attributing some of the "disproportionate" success US tech companies have had (relative to other nation's tech companies) to Section 230 and the DMCA); *id.* at 139 (noting that Wikimedia Foundation's former general counsel has called Section 230 and the DMCA as "essential" to today's internet); *see also* Katherine Trendacosta, *Reevaluating the DMCA*

like Section 230, Section 512 has been criticized. The DMCA's takedown and put-back procedures have been described as an inefficient and ineffective game of "whack a mole."[101] Copyright owners complain that they have to spend valuable time and resources policing the web to see if their own content is being unlawfully shared. Some scholars argue that the safe harbor notice and takedown procedures create too great an incentive for service providers to remove content, even lawful content.[102] Why risk the copyright lawsuit if you are protected by removing the content?

Because it is relatively easy to send a DMCA copyright notice, and because service providers are arguably more incentivized by the safe harbor to remove content than to engage in a potentially costly investigation into the merits of the underlying copyright claim, there is a very real risk that the process can be abused to stifle lawful speech. As one scholar has noted, "[i]f this takedown procedure took place through the courts, it would trigger First Amendment scrutiny as a prior restraint—silencing speech before an adjudication of unlawfulness. But because DMCA takedowns are privately administered through service providers, they have not received such constitutional scrutiny

22 Years Later: Let's Think of the Users, ELEC. FRONTIER FOUND. (Feb. 12, 2020), https://www.eff.org/deeplinks/2020/02/reevaluating-dmca-22-years-later-lets-think-users [https://perma.cc/UKV6-Z9QT] ("Without [Section 512's] safe harbor, the risk of potential copyright liability would prevent many services from doing things like hosting and transmitting user-generated content. Thus the safe harbors, while imperfect, have been essential to the growth of the Internet as an engine for innovation and free expression."); KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST 205 (2018) (noting that Section 512 and Section 230 are the "twin safe harbors from the 1990s" and were "a significant factor in the rapid growth of Internet-based applications"). Werbach notes that these safe harbor provisions were "particularly important to the spread of user-drive Web 2.0 services." *Id.*

[101] *See, e.g.*, Morgan E. Pietz, *Copyright Court: A New Approach to Recapturing Revenue Lost To Infringement: How Existing Court Rules, Tactics From the "Trolls," and Innovative Lawyering Can Immediately Create a Copyright Small Claims Procedure That Solves Bittorrent and Photo Piracy*, 64 J. COPYRIGHT SOC'Y U.S. 1, 4 (2017) (discussing how "the DMCA takedown procedure is seen by content owners as an ineffective and expensive game of whack-a-mole that seldom succeeds in permanently removing infringing content").

[102] *See* Lemley, *supra* note 76, at 115 ("Notice and takedown therefore rewards overzealous copyright owners who use the DMCA mechanism to rid the Web even of legitimate content, secure in the expectation that ISPs will take everything down rather than risk their eligibility for the safe harbor."); *see also* Matthew Schonauer, *Let the Babies Dance: Strengthening Fair Use and Stifling Abuse in DMCA Notice and Takedown Procedures*, 7 I/S: J.L. & POL'Y FOR INFO. SOC'Y 135, 152 (2011) ("[S]ince its enactment, observers of DMCA takedown practices have decried a plethora of uses by rights holders as abuse of the process.").

despite their high risk of error."[103] Critics have also argued that the DMCA has harmed privacy rights and undercut information security.[104]

In 2020, the U.S. Copyright Office completed a comprehensive review of Section 512 and issued a report that was "the first comprehensive study issued by a U.S. government agency on the operation of section 512."[105] That report also concluded that courts have construed the safe harbor provision broadly, perhaps even beyond the bounds Congress meant to protect.[106] The report concluded that "[b]ased on the Office's review of the case law related to the eligibility requirements for the section 512(a), (b), (c), and (d) safe harbors, there is a risk that they, as currently interpreted, may encompass activities and service providers that Congress did not intend to protect under the safe harbors."[107]

At the same time, scholars have noted that Section 512's safe harbor provisions have certain positive features as well. Jonathan Zittrain has written that, although there are certain deficiencies, "[the DMCA] notice-and-takedown regime . . . reflects a balance."[108] Websites have been able to host a wide variety of content, including "amateur expression," and this has allowed for huge growth in the field.[109] At the same time, copyright holders have "a ready means of redress for the most egregious instances of copyright infringement, without chilling individual expression across the board in the process."[110] These takedown and putback procedures separate the Section 512 safe harbor from the Section 230 safe harbor, where there is no obligation on

[103] Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J.L. & TECH. 171, 176 (2010) (arguing that "the copyright notice-and-takedown regime operates in the shadow of the law, silencing speech indirectly through private intermediaries where the government could not do so directly").

[104] *See* Trendacosta, *supra* note 100.

[105] *See* U.S. COPYRIGHT OFF., *supra* note 94, at acknowledgements.

[106] *Id.* at 89 ("The Second and Ninth Circuits, along with their lower courts, have thus broadened the protections of the safe harbors to include services being done 'by reason of' storage of the copyrighted material at the direction of a user. Such a broad interpretation of the activities covered by the section 512(c) safe harbors may result in protecting activities beyond what Congress initially anticipated, and perhaps beyond what Congress intends to protect."); *see also id.* at 90 ("[C]ourts have on occasion applied the section 512(a) safe harbor in an expansive manner, at times in ways likely not within the scope of what Congress intended.").

[107] *Id.* at 94.

[108] ZITTRAIN, *supra* note 4, at 119.

[109] *Id.*

[110] *Id.*

the part of an internet service provider to remove any content.[111] For this reason and other reasons discussed in greater depth in Part IV below, Section 512's safe harbor provisions may ultimately prove a better model than Section 230's.

III. Blockchain Technology

In order to understand how the lessons of early internet regulation might inform blockchain regulation, it is important to understand the historical, cultural, philosophical, and political contexts of the development of blockchain technology. Like early internet, blockchain technology is in part an outgrowth of the philosophical goals and concerns of a committed group of enthusiasts and early adopters. Initial goals of the blockchain community included a drive to protect privacy, a desire to create systems that did not rely on government or other centralized forces, and an attempt to reduce expensive inefficiency. Understanding these goals and how the technology was developed to reach them better informs the considerations for lawmakers included later in the article. This Part will first trace the history of blockchain before providing a layman's overview of the technology itself.

A. History

i. Early Blockchain and the Shift from Typewriters to PCs

Although most people do not associate blockchain technology with word processing, the shift from typewriters to computers is an important part of the inspiration for the technology. The rise of the personal computer dramatically changed the way that serious writing was done. On an obvious level, authors could now store text that would previously have been written on paper on a computer instead. On a less obvious level, this shift to digital created certain issues with document authentication. Computers hold many advantages over physical paper, including that edits can be easily made, and, crucially, there are no or few signs that the final document has been altered. Without the telltale signs of whiteout and literal cuts and pastes, it is less obvious when changes have been made.

[111] "Perhaps the most salient difference between section 512 of the DMCA and section 230 of the CDA is that the latter provision lacks a notice-and-takedown regime. That is, an intermediary that relies upon the protections of section 230 of the CDA is under no obligation to remove defamatory or offensive content after being notified of its existence." Nicholas W. Bramble, *Safe Harbors and the National Information Infrastructure*, 64 HASTINGS L.J. 325, 355 (2013) (footnote omitted).

However, there are times it is desirable to know what changes have been made to a document, by whom, and when. For example, in a copyright infringement dispute where both authors claim to have written a passage, digital proof that one of them had it on their computer prior to the other is quite valuable. Computers *have* the ability to keep a history of all changes to a document, but the means of accessing the list of those changes is often difficult.[112] Further, anyone with access to the computer can delete or modify the list of changes.[113] Thus, a problem: how to easily log all changes to a digital document in a format that is secure, stable, and inspectable?

Two Bell Labs computer science researchers, Stuart Haber and Scott Stornetta, were contemplating this problem in 1990.[114] They developed a system called "secure digital time stamping" that allowed users to maintain most of the tamper-resistant properties of a physical notebook but still store the contents in an entirely digital manner.[115] Their paper, entitled "How to Time Stamp a Digital Document," was the first invention of a blockchain.[116] The system they created provided a way to digitally store the contents of a page such

[112] "[Early personal computers], while powerful, had relatively few applications and were not, despite the advertising copy, user-friendly. . . . Data recovery was a major issue because storage was costly and users routinely deleted data and re-formatted media." Mark Pollitt, *A History of Digital Forensics*, *in* ADVANCES IN DIGIT. FORENSICS VI 3, 6 (2010), https://hal.inria.fr/hal-01060606/document [https://perma.cc/47JK-NR3G].

[113] In their classic paper on the ten most important information security principles, Saltzer and Schroeder state the following about the principle of access control: "Unless the terminal [application], its object reader [processor], and its communication lines to the computer are physically secured against tampering, it is relatively easy for an intruder to modify the terminal to transmit any sequence of bit [they] choose." Jerome Saltzer & Michael Schroeder, *The Protection of Information in Computer Systems*, 63 PROC. INST. ELEC. & ELEC. ENG'R 1278, 1286 (1975), https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a60a942d7e134e10a67d64a1cc245783d649eba6 [https://perma.cc/FT8V-7R9K]. This technique can be used to modify any data on the computer, including documents, log files of changes to documents, and even the log files of instructions run by the system processor also known as the "system event log." There is also a field of computer security research devoted to increasing the security properties of log files that reside on untrusted hardware (hardware that does not have the assumption of logical or physical access control). *See* Bruce Schneier & John Kelsey, *Secure Audit Logs to Support Computer Forensics*, 2 ACM TRANSACTIONS ON INFO. AND SYS. SEC., 159, 171–72 (1999), https://dl.acm.org/doi/abs/10.1145/317087.317089 [https://perma.cc/3KA9-29TC].

[114] Stuart Haber & W. Scott Stornetta, *How to Time-Stamp a Digital Document*, 3 J. CRYPTOLOGY 99, 99 (1991).

[115] *Id.* at 100.

[116] *Id.*

that it could not be altered without easy detection.[117] It also required users to signify that they "signed" the contents of all pages at a specific point in time.[118]

Computers allowed users to easily edit other types of digital content, including drawings, digital paintings, pictures, video, and more.[119] Researchers in communities like information security and auditors saw the value in keeping a full log of all changes made to a digital file.[120] The invention and adoption of internet technologies for file sharing and world wide web technology for publishing led to an explosion of sharing of content of all kinds. Thus, digital change logs across multiple parties became more relevant than ever before.

Nevertheless, when the Haber and Stornetta research paper on blockchains was published in 1991, the technology did not receive much attention.[121] Blockchains add additional cost and overhead to document publishing, and since most applications did not require the tracking and publication of all changes, the extra expense was not viewed as "worth it." The networking and sharing of computers and data was not nearly as prevalent in 1992 as it is today. It was unclear at that time that the origin of information was going to be a widespread problem on the internet, or that trust in institutions would degrade. Thus, the Haber and Stornetta blockchain technology did not receive much notice until a 2008 white paper first proposed a digital currency called Bitcoin.[122]

[117] *Id.* at 109.

[118] *Id.* at 102.

[119] Digital photography was available to some as early as 1991, and artists were experimenting with editing photo media for many decades prior. *See The Time-Travelling Camera: A Short History of Digital Photo Manipulation*, SCI. & MEDIA MUSEUM (June 16, 2021), https://www.scienceandmediamuseum.org.uk/objects-and-stories/digital-photo-manipulation-history [https://perma.cc/MBS6-S8AF].

[120] Carl E. Landwehr, *Computer Security*, 1 INT'L J. INFO. SEC. 3, 9–10 (2001) (commenting on the difficulties of preserving a detail event log of computer system operations due to the large number of operations that occur and potential for attacker manipulation: "[Computer operating system] logs can be used to reconstruct an intruder's activities once the intrusion has been identified, but reviewing the log to determine whether an intrusion has occurred or not is likely to be impractical").

[121] Amy Whitaker, *The Eureka Moment That Made Bitcoin Possible*, WALL ST. J. (May 25, 2018, 1:07 PM), https://www.wsj.com/articles/the-eureka-moment-that-made-bitcoin-possible-1527268025 [https://perma.cc/PK3D-AK9V].

[122] The Haber & Stornetta paper is cited multiple times in the Bitcoin whitepaper. Their system is the basis for the block and chain inspired ledger that is used to track Bitcoin transactions among all participants in Nakamoto's system. SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 2 (2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/7UM5-AM33]; *see also* Whitaker, *supra* note 121 ("When the founding document of bitcoin was published in 2008 under the

ii. Satoshi Nakamoto's White Paper

On Halloween of 2008, the pseudo-anonymous handle "Satoshi Nakamoto" posted a whitepaper on a cryptography mailing list describing a system that allowed for the entirely digital exchange of currency between two individuals.[123] The author named the system "Bitcoin," and subsequently posted code which allowed any individual to participate in the Bitcoin system.[124] The identity of Satoshi Nakamoto has remained a mystery over the years, though one much speculated upon.[125] Satoshi made careful design choices about the Bitcoin system and used results from many decades of research in a variety of topics, including computer science, computer security, privacy, and economics.[126] The work of Haber and Stornetta clearly influenced Satoshi. The Bitcoin white paper cited eight research papers; three were authored by a combination of Haber and Stornetta.[127]

Satoshi's Bitcoin system was more than a mere blockchain or distributed ledger. Rather, it paired a blockchain with other emerging and existing

name 'Satoshi Nakamoto'—a pseudonym for one or more scientists—it had just eight citations of previous works. Three of them were papers co-authored by Drs. Haber and Stornetta.").

[123] WERBACH, *supra* note 100, at 17.

[124] *Id.* at 42 ("In the Bitcoin whitepaper, Satoshi Nakamoto put together cryptographically secured digital cash with a P2P validation network for a shared ledger, adding a few elegant tweaks along the way. Over the subsequent months, he engaged in online dialogues with digital cash afficionados. They quickly produced software code that could implement the concepts described in the paper."); *see also* ARVIND NARAYANAN, JOSEPH BONNEAU, EDWARD FELTEN, ANDREW MILLER & STEVEN GOLDFEDER, BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION 176 (2016) (describing the Bitcoin whitepaper and noting that "[o]pen-source software implementing [Bitcoin's technical design and philosophy] . . . was released soon after").

[125] *See* NARAYANAN, BONNEAU, FELTEN, MILLER & GOLDFEDER, *supra* note 124, at XXIII (noting that Satoshi Nakamoto is a pseudonym adopted by the creator of bitcoin and speculating upon his still unknown identity).

[126] Arvind Narayanan & Jeremy Clark, *Bitcoin's Academic Pedigree*, 60 COMMC'NS ASS'N COMPUTING MACH. 36, 36 (2017) (describing that "nearly all of the technical components of bitcoin originated in the academic literature of the 1980s and 1990s").

[127] NAKAMOTO, *supra* note 122, at 9. Two of the papers were iterations of the digital time stamping invention (i.e., blockchain) and the third was on making the output of one-way hash functions more usable for finding information. Bitcoin used this in how addresses are generated instead of allowing users to choose usernames. *See* Narayanan & Clark*, supra* note 126, at 45 (citing Haber & Stornetta, *supra* note 114, at 99); Dave Bayer, Stuart Haber & W. Scott Stornetta, *Improving the Efficiency and Reliability of Digital Time-Stamping*, *in* SEQUENCES II: METHODS IN COMMUNICATION, SEQUENCING, AND COMPUTER SCIENCES 329, 329–34 (Renato Capocelli & Alfredo De Santis Ugo Vaccaro, eds., 1993); Stuart Haber & W. Scott Stornetta, *Secure Names for Bit-Strings*, *in* PROCEEDINGS OF THE 4TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 28, 28–35 (1997).

technologies.[128] It combined a peer-to-peer network, a public software client, and a mechanism and protocol to determine consensus among a decentralized group of participants (consensus and its role in blockchain is explained in greater detail below)[129] with tradeoffs that users were willing to accept.[130] Crucially, the Bitcoin system also involved a way to incentivize network participants for their activity (mining, also explained below).[131] These features helped solve the problem of how to build trust in a pseudonymous system by incentivizing a way to get most of the network participants to behave honestly most of the time. The Bitcoin system also included a way for new nodes to join the network,[132] and used a blockchain to store the entire agreed upon history of all Bitcoin transaction activity in a tamper-evident way.[133]

The Bitcoin system was reflective of many ideas posted to a mailing list and message board maintained by a group of crypto-libertarians who named themselves the "cypherpunks."[134] "Cypherpunks were activists who opposed the power of government and centralized institutions, and sought to create social and political change through cryptography."[135] The cypherpunks embraced the digital libertarian ethos of highly valuing privacy and using

[128] *See* Narayanan & Clark, *supra* note 126, at 42 (describing time stamping and other bitcoin features and noting "Nakamoto's genius, then, was not any of the individual components of bitcoin, but rather the intricate way in which they fit together to breathe life into the system").

[129] *See infra* Section III.B.

[130] *See* NARAYANAN, BONNEAU, FELTEN, MILLER & GOLDFEDER, *supra* note 124, at XXVI ("Bitcoin has several notable innovations, including the [public] block chain and a decentralized model that supports user-to-user transactions. It provides a practically useful but less than perfect level of anonymity for users."); *id.* at XXVII ("Bitcoin, in retrospect, seems to have made the right compromises. It scales back anonymity a bit and requires participants to be online and connected to the peer-to-peer network, which turned out to be acceptable to users.").

[131] *See infra* Section III.B.

[132] *See* Narayanan & Clark, *supra* note 126, at 40 ("[Nakamoto] uses some concepts [from the research field of fault-tolerant distributed systems], referring to his protocol as a consensus mechanism and considering faults both in the form of attackers, as well as nodes joining and leaving the network.").

[133] *See id.* at 38 ("A [succinct cryptographic] digest is a short string that makes it possible to avoid storing the entire ledger, knowing that if the ledger were tampered with in any way, the resulting digest would change, and thus the tampering would be detected.").

[134] Haseeb Qureshi, *The Cypherpunks*, NAKAMOTO (Dec. 29, 2019), https://nakamoto.com/the-cypherpunks/ [https://perma.cc/AZ9Y-HR3D]. For an archive of emails and postings to the cypherpunks mailing-list between 1992 and 1999, see *Cypherpunks Mailing List Archive*, CRYPTO ANARCHY, https://mailing-list-archive.cryptoanarchy.wiki/ [https://perma.cc/V62E-QAL3].

[135] *See* Narayanan & Clark, *supra* note 126, at 41.

technology to shield speech from government intrusion and censorship.[136] They were skeptical of government[137] and highly centralized industries like banking.[138] Building a payment network that was decentralized was a longstanding goal of the cypherpunk community.[139]

Cypherpunks cared about a variety of philosophical issues raised by technology, including the private nature of physical cash transactions, the personal information required by e-commerce and credit card transactions, the aggregation of consumer data, and the potential for abuse of consumer trust by organizations who collect their data.[140] The relatively large-scale adoption of Bitcoin, as opposed to other digital currency projects that came before it, was in part due to its responsiveness to these concerns. Bitcoin allowed its users access to a digital currency without the need for identification (a pseudonymous system) and free of any specter of regulation or control from a centralized entity (often referred to as "censorship resistance").[141]

[136] *Id.* at 43.

[137] *See* NARAYANAN, BONNEAU, FELTEN, MILLER & GOLDFEDER, *supra* note 124, at 175 (discussing how, with the help of cryptography, "cypherpunks believed" that "people could protect themselves and their [private] interests more effectively and with much less activity by (or, as they would say, interference from) government").

[138] David Chaum, *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*, 28 COMMC'NS ASS'N COMPUTING MACH. 1030, 1030 (1985). The author first notes in the introduction that "[t]he foundation is being laid for a dossier society, in which computers could be used to infer individuals' life-styles, habits, whereabouts, and associations from data collected in ordinary consumer transactions." *Id.* The author then uses the rest of the paper to present a system for performing electronic payments that would not be traceable by banks even if they were cooperating with each other to perform tracking. *See id.* at 1030–44.

[139] *See* NARAYANAN, BONNEAU, FELTEN, MILLER & GOLDFEDER, *supra* note 124, at 175 ("One of the challenges in the cyperpunk movement was how to deal with money . . . ."); *see also* David Chaum, *Blind Signatures for Untraceable Payments*, *in* 82 ADVANCES IN CRYPTOLOGY: PROCEEDINGS OF CRYPTO 199, 199 (1983) (discussing the challenge of how to deal with the criminal element that untraceable money would inevitably attract). "The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use of payments. Ideally a new payments system should address both of these seemingly conflicting sets of concerns." *Id.*

[140] *See* Chaum*, supra* note 138, at 1030 ("Uncertainty about whether data will remain secure against abuse by those [organizations] maintaining or tapping it can have a 'chilling effect' [on consumer behavior]."); *see also id.* ("[O]rganizations are [still] vulnerable to abuses by individuals.").

[141] Rainey Reitman, *Bitcoin - A Step Toward Censorship-Resistant Digital Currency*, ELEC. FRONTIER FOUND. (Jan. 20, 2011), https://www.eff.org/deeplinks/2011/01/bitcoin-step-toward-censorship-resistant [https://perma.cc/92UB-57VV].

B. The Technology

A basic lay person's understanding of blockchain technology is quite helpful to contextualize the challenges lawmakers will face in regulating it. Bear in mind the philosophical goals of the cypherpunks and early blockchain enthusiasts: privacy, decentralization, and reduced inefficiency, among others. These philosophical goals informed the technological development of blockchain.

The easiest way to understand the technology is by way of analogy. Cryptocurrency is currently the most recognizable application of blockchain, and so a bank account analogy is an accessible one. In a traditional banking scenario, a customer opens an account with a bank, which is, of course, a centralized entity. Banking regulations, including U.S. "Know Your Customer" laws and anti-money laundering laws, require banks to collect specific information about any person who wishes to open an account.[142] The customer's account balance is kept in a bank book with a digital copy stored on servers the bank controls. The bank processes and verifies all of the deposits and debits the customer makes and records the results in the book. If the customer wants to remove money from their account, the bank will require some sort of verification that (1) the customer is indeed the account holder and (2) the account contains sufficient funds for the transaction. If the customer wishes to send a third-party money, the customer has to provide their bank with the recipient's name and account information. The bank has to verify that the customer does indeed have the amount they are requesting to send. The account balance and transaction history are maintained by the bank, and if the customer wishes to view it, they go through the bank. Generally, only the customer, bank employees, and anyone the customer authorizes can view the customer's banking records. The bank usually also employs a reputable third-party audit firm to check that the books are updated properly. A person who dislikes a centralized agency being able to view their financial data and is resistant to being under the thumb of government regulation will chafe at these banking requirements.

[142] Marguerite Colson & Eric Van Nostrand, *Sanctions that Sting: Private Sector Solutions to the Paper Tiger Problem*, 32 YALE J. ON REG. 561, 579 (2015) ("Before opening accounts for new clients, banks conduct rigorous background investigations, performing Know Your Customer (KYC) and Anti-Money Laundering (AML) checks.").

With blockchain, the bank account is replaced with a distributed electronic ledger. Although the term "blockchain" resists simple definitions,[143] it is enough for the purposes of this Article to say that it refers to the units of data which are assembled into a block. Each block is then linked or "chained" to another block, with the result being that their order is locked in place: you can always know which block came before a certain block and which block comes after a certain block. The data in the blocks can be anything (for example text, images, video, and more), and some applications of blockchain do not involve cryptocurrencies.[144] For our analogy, and in the Bitcoin system, the data stored in the blocks is the amount of cryptocurrency users send to each other.

In our blockchain scenario, there is no centralized bank that stores and verifies account amounts. Rather, the amount of each users' cryptocurrency holding is stored on the networks by many other users; any user can have a copy of the entire history of all transactions. Each person who has access to the blockchain can know exactly how much currency every other user has, and so no one would enter into a transaction with a person who did not have enough currency. Instead of having users choose usernames or using their real name, the software generates an address for them to use instead, using public key cryptography, which is explained below. There is no centralized agency which a user must submit their name and information to. Anyone who wishes to participate can simply download the software.

[143] "[T]he term *blockchain* has no standard technical definition but is a loose umbrella term used by various parties to refer to systems that bear varying levels of resemblance to bitcoin and its ledger." Narayanan & Clark, *supra* note 126, at 43; s*ee also* Michele Benedetto Neitz, *How to Regulate Blockchain's Real-Life Applications: Lessons from the California Blockchain Working Group*, 61 JURIMETRICS J. 185, 190 (2021) ("[T]he word 'blockchain' does not have a commonly understood definition.").

[144] Elizabeth Paton, *LVMH, Richemont and Prada Unite Behind a Blockchain Consortium*, N.Y. TIMES (Apr. 20, 2021), https://www.nytimes.com/2021/04/20/business/lvmh-richemont-prada-blockchain.html [https://perma.cc/2LA8-PHPF] (describing the Aura blockchain for luxury goods); *see also* Kate Vitasek, John Bayliss, Loudon Owen & Neeraj Srivastava, *How Walmart Canada Uses Blockchain to Solve Supply-Chain Challenges*, HARV. BUS. REV. (Jan. 5, 2022), https://hbr.org/2022/01/how-walmart-canada-uses-blockchain-to-solve-supply-chain-challenges [https://perma.cc/3XAC-XUTA] (announcing Walmart Canada's use of a blockchain to manage parts of their supply chain); Adam Kress, *Honeywell Uses Blockchain to Digitize Aircraft Records, Parts Pedigree Data*, HONEYWELL (Aug. 4, 2020), https://www.honeywell.com/us/en/press/2020/08/honeywell-uses-blockchain-to-digitize-aircraft-records-parts-pedigree-data [https://perma.cc/EZ2Z-9F6L] (announcing Honeywell's use of a blockchain for tracking certain aircraft parts).

The system is thus decentralized and allows for privacy. In order to guard against a malicious actor who will simply try to rewrite the ledger to give themself more currency than they actually have, the system uses certain technological safeguards. How do you make sure that the copy of the ledger that is stored is the same copy across all network users? There is a special process that is written into the software, an algorithm that determines who is allowed to add a new block to the chain. In Bitcoin, that process is called "mining," and the Bitcoin client software has a special puzzle that the "miner" has to solve.[145] If they solve that puzzle correctly, they can create a new block.[146] All of this was outlined in the Bitcoin white paper and implemented in code.[147]

If you do not know the other people on the Bitcoin system, how can you keep somebody from logging into your account on the blockchain and accessing things in your name? The answer was to use two other technologies that work together called public key cryptography and digital signature. In public key cryptography, you generate a key pair, which is one public key and one private key. These keys are mathematically linked together. Using digital signature, you can send messages that have been signed with your private key and anyone who has a copy of your public key can verify that your private key was used to sign the message.[148]

Thus, in a cryptocurrency example, the bank book is replaced by a blockchain and used to record all deposits and debits. The customer account number is replaced with their public key and the customer signature is replaced by their private key. Any proposed transactions that are signed correctly by the private key can be verified by any other user. With the Bitcoin protocol, it was possible to have a currency that pseudonymous users could exchange without the need for a centralized authority. The next generation of blockchain applications would involve creating new protocols that expanded the choices of what users could send.

[145] Narayanan & Clark, *supra* note 126, at 42.

[146] *Id.*

[147] *See* NARAYANAN, BONNEAU, FELTEN, MILLER & GOLDFEDER, *supra* note 124, at 202.

[148] Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, 22 INST. ELEC. & ELEC. ENG'R TRANSACTIONS ON INFO. THEORY 644, 649 (1976) (introducing the required properties of a digital signature that can be used to send messages over "public" computer networks such as the internet).

C. Continued Evolution: Ethereum and Smart Contracts

The Bitcoin software program demonstrated that it was possible to build a network that satisfied decentralization goals because it could be operated without a centralized authority and without any "middlemen." Further, the Bitcoin program established that users would voluntarily operate the network using cryptocurrency as the incentive. Although Bitcoin demonstrated that a new type of decentralized network was possible on the internet, its features were largely limited to allowing users to exchange amounts of Bitcoin with each other. However, that would soon change, as early adopters of Bitcoin found ways to leverage certain fields in the Bitcoin protocol to exchange data with each other. [149]

Developers began to modify and remix the Bitcoin client software resulting in new software that runs new blockchain ledgers and new kinds of cryptocurrency coins. The most successful new cryptocurrency project was called Ethereum. Ethereum created software to enable many more types of instructions to be run during a transaction while still recording all history to a blockchain.[150] They called this part of the software the "Ethereum Virtual Machine" or EVM. The EVM allowed network users to execute their own customized instructions during transactions and pay for the computation costs using their cryptocurrency.[151] This resulted in the ability for anyone to build and use "smart contracts" on the Ethereum network.[152]

In essence, the term smart contracts (which may not be contracts at all)[153] refers to the ability to automate the specification and execution of traditional

[149] *See* NARAYANAN, BONNEAU, FELTEN, MILLER & GOLDFEDER, *supra* note 124, at 79, 82.

[150] *Id.* at 285–86.

[151] *Id.* at 264–65 ("Anybody can create an Ethereum contract, for a small fee, by uploading its program code in a special transaction.").

[152] *Id.* at 265 (noting that once contracts are built, they can be used by anyone on the network without additional owner actions); *id.* ("Once uploaded, the contract will live on the block chain. It has its own balance of funds, other users can make procedure calls through whatever the [application programmer interface] exposes, and the contract can send and receive money.").

[153] In their 2017 article, Kevin Werbach and Nicolas Cornell discuss the ways "smart contracts" are different from traditional contracts. Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313, 339–40 (2017). "In a very real way, smart contracts are not intended to be legally enforceable. . . . This lack of intent may lead to the conclusion that, even conceptually, smart contracts are not truly contracts at all." *Id.* "They may look more like so-called 'gentlemen's agreements,' intended to be carried out, but never intended to reach a courtroom. This appearance would be misleading, however, because it is quite different to intend that a solution will not be needed than to intend that it will be unavailable." *Id.*

contracts via computer instructions (essentially, algorithms).[154] The researcher who coined the term, Nick Szabo, noted that they were intended to "[f]ormalize and secure digital relationships" but to do so in a manner that is much more "[f]unctional" than paper-based contracts.[155] An analogy that Szabo used for digital smart contracts is that they would be similar to digital vending machines.[156] The machine would be pre-loaded with a variety of items that it could provide, and it would autonomously await payment and the user's selection before executing or delivering the items to the user. Typically, payment is returned if the network is unable to execute the contract instructions, but it is not always clear how other kinds of disputes will be handled.[157]

Smart contracts on Ethereum are provided a special status. A smart contract is given a set of instructions, its own address, and thus its own account balance.[158] Nearly all contracts are intended to be autonomous. The contract's logic (software instructions) dictates how the contract will send or receive funds based upon certain other events. For example, two users could create a contract that pays the first user if the temperature on a certain future date is above a specific number, otherwise it pays the other user. Both users can inspect the logic of the contract since it is published on a public blockchain, and the contract automatically executes on the date without human intervention (it receives the weather from a mutually agreed upon data feed and sends funds

[154] NICK SZABO, SMART CONTRACTS: BUILDING BLOCKS FOR DIGITAL MARKETS 1 (1996), https://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf [https://perma.cc/XX2D-LAK7] ("The basic idea of smart contracts is that many kinds of contractual clauses (such as liens, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher.").

[155] Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 2 FIRST MONDAY (1997), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/formalize.html [https://perma.cc/5VXX-RQC2] ("Smart contracts utilize protocols and user interfaces to facilitate all steps of the contracting process. This gives us new ways to formalize and secure digital relationships which are far more functional than their inanimate paper-based ancestors.").

[156] SZABO, *supra* note 154.

[157] Stuart D. Levi & Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, HARV. L. SCH. F. ON CORP. GOVERNANCE (May 26, 2018), https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations [https://perma.cc/F2Y3-XJ2P] ("Thus, although smart contracts will render payments far more efficient, they may not eliminate the need to adjudicate payment disputes.").

[158] NARAYANAN, BONNEAU, FELTEN, MILLER & GOLDFEDER, *supra* note 124, at 287.

accordingly).[159] Smart contracts have limits when compared to paper-based contracts, but for narrow types of transactions they can represent a significant increase in contract execution speed[160] and in providing a shared public record of events.[161] Other cryptocurrency projects have also attempted to launch new currency and blockchain networks with additional features such as faster transaction speeds, higher transaction volumes, etc., but none have yet become as widely used as Bitcoin or Ethereum.

The most popular use of smart contracts today is in the creation of other kinds of digital tokens, such as Non-Fungible Tokens (NFTs).[162] To build an NFT, a developer creates a contract that itself has a function to make new tokens. Other users can send the contract their cryptocurrency funds and the contract will autonomously create a new token and record the owner of that token onto the network's blockchain. If the owner of the token wants to transfer or sell their token to another user, they just need to send an instruction to the autonomous smart contract.[163] The new token owner is recorded on the blockchain. Since the contracts and the blockchain network they run on are always available, transactions such as ownership changes or creating new

[159] Scholars have noted that blockchain applications like smart contracts are ironically akin in many ways to the legal system. "While it seemingly precludes traditional legal enforcement, a blockchain-based system's software enforces its own rules in a manner analogous to the legal system. It thus illustrates the foundational insight of cyberlaw scholar Lawrence Lessig's 1999 book, *Code and Other Laws of Cyberspace*: code is law." Werbach, *supra* note 10, at 492.

[160] *See* Levi & Lipton, *supra* note 157 ("Smart contracts are presently best suited to execute automatically two types of 'transactions' found in many contracts: (1) ensuring the payment of funds upon certain triggering events and (2) imposing financial penalties if certain objective conditions are not satisfied.").

[161] This property is not specifically mentioned in the early smart contract literature. Instead, it comes from the hosting of the smart contract on a publicly accessible blockchain such as Ethereum. The blockchain ledger records a public append-only record of all transactions between all users and all smart contracts thus providing a full audit trail of events. *See* Shafaq Naheed Khan, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa & Anoud Bani-Hani, *Blockchain Smart Contracts: Applications, Challenges, and Future Trends*, 14 PEER-TO-PEER NETWORKING & APPLICATIONS 2901, 2901 (2021).

[162] A non-fungible token usually means there is only one of the token and unlike a cryptocurrency, its value or the item that it links to is usually not the same as any other item. They have been referred to as a way to introduce the concept of scarcity into digital environments which is a fairly new idea because copies of a digital item can be made for nearly no cost. However, this point is somewhat debated. *See* Jonathan Zittrain & Will Marks, *What Critics Don't Understand About NFTs*, ATLANTIC (Apr. 7, 2021), https://www.theatlantic.com/ideas/archive/2021/04/nfts-show-value-owning-unownable/618525/ [https://perma.cc/E4A5-B952].

[163] NARAYANAN, BONNEAU, FELTEN, MILLER & GOLDFEDER, *supra* note 124, at 265 (explaining how users can interact with smart contracts using a simple example).

tokens are not restricted to traditional execution limitations such as weekdays, trading hours, market hours, working hours, etc.[164] It is often very expensive to store full data on a blockchain such as Ethereum, so most tokens contain a reference to the data stored elsewhere rather than the actual data.[165] For example, the tokens might contain a link to other digital materials posted by the creator on an external website such as a video, text file, or image.

Companies from a variety of industries are starting to evaluate and experiment with smart contracts, including auctions,[166] art,[167] finance,[168] real

[164] Eva Szalay, *Crypto Trading Puts Pressure on Bourses to Open All Hours*, FIN. TIMES (Nov. 14, 2021), https://www.ft.com/content/7b7ff0cb-b695-485d-b6be-ef0c8c0edde0 [https://perma.cc/Y3KC-KYW9] (explaining that the non-stop trading of cryptocurrency was influencing the trading hours of bourse/stock exchange markets).

[165] *See* NARAYANAN, BONNEAU, FELTEN, MILLER & GOLDFEDER, *supra* note 124, at 288; Clive Thompson, *The Untold Story of the NFT Boom*, N.Y. TIMES (May 12, 2021), https://www.nytimes.com/2021/05/12/magazine/nft-art-crypto.html [https://perma.cc/CJ6E-RFQV].

[166] Christie's has launched their own digital auction market platform dedicated to NFT-based art called "Christies 3.0." *Digit. Art & NFTs*, CHRISTIE'S, https://www.christies.com/en/events/digital-art-and-nfts/overview [https://perma.cc/6MYA-8DXA].

[167] Amy Whitaker, *Art and Blockchain: A Primer, History, and Taxonomy of Blockchain Use Cases in the Arts*, 8 ARTIVATE 27, 29 (2019) ("[T]he developments in blockchain since the early 1990s may, in a relatively short time, have profound implications for art historians, artists, conservators, collectors, dealers, museums, and broader ecosystems of cultural assets and creative industries.").

[168] Kevin Roose, *The Latecomer's Guide to Crypto*, N.Y. TIMES (Mar. 18, 2022), https://www.nytimes.com/interactive/2022/03/18/technology/cryptocurrency-crypto-guide.html [https://perma.cc/BX6J-RW4C].

estate,[169] fast food,[170] clothing,[171] wine,[172] spirit making,[173] and more.[174] Some projects are meant to attract new customers or create new ways of transacting with customers. Others are looking at new business models, new technology enablers for business, or opportunities to reduce transaction costs. The technology provides an alternative for buyers and sellers who are not satisfied with the traditional system. Whether the technology's disadvantages outweigh its advantages is a topic of much current debate.[175] As the applications of blockchain technology continue to grow, and especially as the money invested in the projects continues to accrue, calls for regulation will also continue to grow louder, as the next section explores.

[169] Kristi Waterworth, *Investing in NFT Real Estate*, MOTLEY FOOL (May 16, 2023, 10:32 AM), https://www.fool.com/investing/stock-market/market-sectors/financials/non-fungible-tokens/nft-real-estate/ [https://perma.cc/FU88-37KV].

[170] *Chipotle Encourages Fans To "Buy the Dip" With New $200,000+ Crypto Game And 1-Cent Guacamole For National Avocado Day*, CHIPOTLE MEXICAN GRILL (July 25, 2022), https://newsroom.chipotle.com/ [https://perma.cc/Q6HT-VW8V] ("Fans can score free Bitcoin, Ethereum, Avalanche, Solana, or Dogecoin and use their crypto to buy real food at Chipotle.").

[171] Jacob Kastrenakes, *Adidas is Launching an NFT Collection with Exclusive Access to Streetwear Drops*, VERGE (Dec. 16, 2021, 2:50 AM), https://www.theverge.com/2021/12/16/22822143/adidas-nft-launch-into-the-metaverse-price-release-date [https://perma.cc/4DVH-NU2F].

[172] Mike DeSimone & Jeff Jenssen, *NFTs Have Arrived in the Wine Industry*, FORBES (Sept. 1, 2021, 9:22 AM), https://www.forbes.com/sites/theworldwineguys/2021/09/01/nfts-have-arrived-in-the-wine-industry/?sh=22091773db39 [https://perma.cc/GP7A-8Q66].

[173] Kara Newman, *The Whiskey Unicorn Goes Crypto*, PUNCH (Oct. 21, 2021), https://punchdrink.com/articles/whiskey-unicorn-goes-crypto-fine-wine-spirits-nfts/ [https://perma.cc/ZL27-7DHT] (explaining that spirit companies have begun to offer NFTs to customers either as digital collectables or in some cases, as a digital right to claim a specific rare physical bottle from the company).

[174] Romain Dillet, *Luxury Watch Maker Breitling Issues Digital Certificates on the Ethereum Blockchain*, TECHCRUNCH (Oct. 15, 2020, 4:44 AM), https://techcrunch.com/2020/10/15/luxury-watch-maker-breitling-issues-digital-certificates-on-the-ethereum-blockchain/ [https://perma.cc/F2KN-8EBC].

[175] *See, e.g.*, Michael J. Casey & Paul Vigna, *In Blockchain We Trust*, MIT TECH. REV. (Apr. 9, 2018), https://www.technologyreview.com/2018/04/09/3066/in-blockchain-we-trust/ [https://perma.cc/VNR3-QXMD]; Stephen Diehl, *Web3 is Bullshit*, STEPHEN DIEHL, https://www.stephendiehl.com/blog/web3-bullshit.html [https://perma.cc/FQV8-DQSE].

IV. APPLYING THE LESSONS OF INTERNET REGULATION TO BLOCKCHAIN

Mark Twain is frequently credited with the saying that "history doesn't repeat itself, but it often rhymes."[176] Today blockchain is in a position similar to that of early internet in the mid-1990s. Both have been heralded as theoretically providing more democratic access and less bureaucratic, centralized involvement. And yet despite increased adoption of blockchain technology, many users find themselves today where early internet users were twenty-five years ago: cautious about using the technology due to fear of fraud, theft, or lack of experience. Recent high-profile indictments for cryptocurrency fraud[177] and market manipulation[178] add to this sense of uncertainty. Thus, increased calls for regulation[179] (regulation that is, of course, counter to the cypherpunk cyberlibertarian ideals).[180]

In responding to these calls, today's lawmakers do not have to draft blockchain regulation from a totally clean slate. Rather, they can and should look to lessons learned from the decades-long implementation of Section 230 and Section 512. This Part looks at the calls for a blockchain safe harbor and discusses how common such safe harbors can be in technology regulation.

[176] *See, e.g.*, Alley v. U.S. Dep't of Health & Hum. Servs., 590 F.3d 1195, 1197 (11th Cir. 2009) ("This aphorism, or one like it, is often attributed to Mark Twain, although there is doubt about whether he is the author of it.").

[177] *See, e.g.*, David Yaffe-Bellany, Matthew Goldstein & Emily Flitter, *Prosecutors Say FTX Was Engaged in a 'Massive, Yearslong Fraud'*, N.Y. TIMES (Dec. 13, 2022), https://www.nytimes.com/2022/12/13/business/ftx-sam-bankman-fried-fraud-charges.html [https://perma.cc/C4XK-4UG3] (quoting Damian Williams, the U.S. Attorney for the Southern District of New York, describing cryptocurrency exchange FTX as "one of the biggest financial frauds in American history").

[178] *See, e.g.*, Press Release, U.S. Att'y Off. S.D.N.Y., Alleged Perpetrator Of $100 Million Crypto Market Manipulation Scheme To Make Initial Appearance In The Southern District Of New York (Feb. 2, 2023), https://www.justice.gov/usao-sdny/pr/alleged-perpetrator-100-million-crypto-market-manipulation-scheme-make-initial [https://perma.cc/Z6V6-EQVC] (describing indictment for commodities fraud and market manipulation in connection with the alleged manipulation of a decentralized cryptocurrency exchange).

[179] For example, four Biden Administration officials recently termed 2022 a "tough year for cryptocurrencies" and urged Congress to "step up its efforts" and "expand regulators' powers to prevent misuses of customers' assets." Brian Deese, Arati Prabhakar, Cecilia Rouse & Jake Sullivan, *The Administration's Roadmap to Mitigate Cryptocurrencies' Risks*, WHITE HOUSE (Jan. 27, 2023), https://www.whitehouse.gov/nec/briefing-room/2023/01/27/the-administrations-roadmap-to-mitigate-cryptocurrencies-risks/ [https://perma.cc/ZQ5Q-6XTK].

[180] NARAYANAN, BONNEAU, FELTEN, MILLER & GOLDFEDER, *supra* note 124, at 188 (discussing regulation of Bitcoin and noting that it is contrary to cypherpunk ideas but concluding "[i]f Bitcoin is big enough to matter, then it is big enough to be regulated," and noting that regulation is already starting to happen).

Ultimately, we are not yet convinced that a safe harbor is appropriate for blockchain technology, and indeed fear that a poorly crafted safe harbor could ultimately harm consumers. We recognize, however, that there may be many reasons lawmakers ultimately choose to include a safe harbor provision in blockchain regulation. Thus, this Part also examines certain considerations that regulators should bear in mind before drafting any blockchain regulation, and includes certain best practices that have emerged for safe harbors.

A. A Safe Harbor for Blockchain?

i. Calls for a Crypto Safe Harbor

Today, blockchain technology faces many of the same challenges the internet faced in 1996. Now, as then, the technology is being deployed in a relative regulatory vacuum. Now, as then, many members of Congress have a limited understanding of the technology and its potential for disruption.[181] Now, as then, certain people are advocating for a safe harbor provision that will allow the technology to continue to develop without being overwhelmed by legal liability.[182]

For example, former Assistant Secretary of Treasury Greg Zerzan has argued that the greatest threat to crypto is regulatory uncertainty and that it thus needs a safe harbor provision like Section 230.[183] Researchers at Coin Center, a non-profit research and advocacy center that focuses on blockchain, have written that "blockchain technologies deserve the same solution and policy approach that the early Internet enjoyed" under Section 230.[184] These proposals

[181] *See, e.g.*, Neitz, *supra* note 143, at 193 ("Blockchain technology can be complicated and intimidating, and few lawmakers have training in computer science.").

[182] Blockchain, and especially cryptocurrencies, do currently face legal actions from government agencies like the FTC and SEC, and the legal landscape continues to evolve. In a recent case the SEC brought against cryptocurrency company Ripple over its token, the court ruled that some aspects of Ripple's token sales met the standard of an investment contract but other aspects did not. SEC v. Ripple Labs, Inc., No. 20 Civ. 10832 (AT), 2023 WL 4507900, at *4 (S.D.N.Y. July 13, 2023). Advocates hoping for total regulatory clarity will have to continue to wait.

[183] Greg Zerzan, *Crypto Needs a Section 230*, INSIDE SOURCES (Apr. 19, 2022), https://insidesources.com/crypto-needs-a-section-230/ [https://perma.cc/M4DX-FRUT] ("Now, cryptocurrency needs this same kind of visionary thinking [that Sec. 230 represents] — a law to protect it from overzealous regulators and ill-fitting old laws.").

[184] Peter Van Valkenburgh, *Congress Should Create a Blockchain Technology Safe Harbor. Luckily They Already Figured it Out in the '90s.*, COIN CTR. (Apr. 6, 2017), https://www.coincenter.org/congress-should-create-a-blockchain-technology-safe-harbor-luckily-they-already-figured-it-out-in-the-90s/ [https://perma.cc/55NL-JPWD] ("CDA 230 was a simple and

join other proposals for some sort of safe harbor protection for crypto, including one by an SEC commissioner.[185] Commissioner Hester M. Peirce has proposed a safe harbor provision that "seeks to provide network developers with a three-year grace period within which, under certain conditions, they can facilitate participation in and the development of a functional or decentralized network, exempted from the registration provisions of the federal securities laws."[186] Commissioner Peirce's proposal is limited to a three-year grace period, an important feature that will be discussed below in the Section on sunset provisions.[187]

In September of 2022, Senator Bill Hagerty of Tennessee proposed a digital asset[188] safe harbor bill when he introduced the "Digital Trading Clarity Act of 2022."[189] Senator Haggerty's bill "provides digital asset exchanges with a safe harbor from certain [SEC] enforcement actions, providing clarity around the classifications of digital assets and applicable liabilities under existing securities laws without sacrificing consumer protection."[190] Senator Hagerty's

elegant legislative solution that enabled Internet businesses to flourish in the US and guaranteed that Internet users would always have a platform from which to share their diverse and expressive content. . . . Why mess with success? It's now time for blockchain technology to get the 230-treatment as well.").

[185] Statement, Hester M. Peirce, Comm'r, SEC, Token Safe Harbor Proposal 2.0 (Apr. 13, 2021), https://www.sec.gov/news/public-statement/peirce-statement-token-safe-harbor-proposal-2.0 [https://perma.cc/USF6-MKVQ].

[186] *Id.* The proposal also notes that "[t]he safe harbor is designed to protect Token purchasers by requiring disclosures tailored to the needs of the purchasers and preserving the application of the anti-fraud provisions of the federal securities laws to Token distributions by an Initial Development Team relying on the safe harbor." *Id.* One of Peirce's fellow SEC Commissioners has criticized the proposal. In an October 21, 2021 speech, Commissioner Caroline A. Crenshaw spoke out against a safe harbor for digital assets. Caroline A. Crenshaw, Comm'r, SEC, Digital Asset Securities – Common Goals and a Bridge to Better Outcomes (Oct. 21, 2021), https://www.sec.gov/news/speech/crenshaw-sec-speaks-20211012 [https://perma.cc/4W97-4RMM].

[187] *See infra* Section IV.B.1.

[188] Both commissioner Pierce and Senator Haggerty use the term "Digital Asset" in their proposals. The IRS defines digital assets broadly as "any digital representation of value which is recorded on a cryptographically secured distributed ledger or any similar technology." *Digital Assets*, IRS, https://www.irs.gov/businesses/small-businesses-self-employed/digital-assets [https://perma.cc/5HYR-LF3P]. In other words, Digital Assets can refer to anything stored on a blockchain, including cryptocurrencies and NFTs. *See id.*

[189] Press Release, Senator Bill Hagerty, Hagerty Introduces Legislation to Provide Crucial Regulatory Clarity for Digital Assets (Sept. 29, 2022), https://www.hagerty.senate.gov/press-releases/2022/09/29/hagerty-introduces-legislation-to-provide-crucial-regulatory-clarity-for-digital-assets/ [https://perma.cc/BZV6-PZKX].

[190] *Id.*

arguments for a safe harbor for digital assets echo the earlier arguments made in favor of Section 230 and Section 512, including that the safe harbor will remove regulatory uncertainty and allow U.S. companies engaged in a "transformational technology" to thrive "at a crucial time."[191]

ii. Safe Harbors are Common in Technology Regulation

It is not surprising that there are multiple calls for a safe harbor for blockchain, and especially for cryptocurrencies.[192] It is quite common for government to encourage safe harbor provisions in other areas of technology. For example, it is a cybersecurity best practice for outside researchers to expose software vulnerabilities by trying to exploit weaknesses (by, for example, attempting to gain unauthorized access to servers). When outside researchers find and report these weaknesses, it allows the companies or agencies that manage the software to "patch" it before it can be exploited by malicious actors. But the outside researchers may be disincentivized by threats of litigation (or worse, as the testing itself may arguably be termed unlawful "computer abuse").[193] In order to encourage researchers to engage in this testing, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued guidance encouraging multiple governments agencies and software companies to adopt

[191] *Id.* (arguing that regulatory uncertainty "discourages investment and job creation here in America and jeopardizes the United States' leadership in this transformational technology at such a crucial time"). Senator Hagerty also argued that his safe harbor provision "is an important step toward providing digital asset intermediaries with much-needed certainty and removing the barriers to entry currently impeding the growth and liquidity of U.S. cryptocurrency markets." *Id.*

[192] Of course, to the extent the SEC is interested in potentially regulating cryptocurrencies, it is worth noting that safe harbor provisions are also found in securities regulation. For example, the Private Securities Litigation Reform Act of 1995 included a "forward-looking statements" safe harbor provision. The intent of that provision was to encourage corporate managers to provide more information to the investing public. "Thus the Act immunizes some issuer statements with a 'safe harbor.' Corporate managers who utilize the Act's safe harbor can now more candidly disclose their plans and projections, without fear of providing 'grist for the litigation mill.'" Ann Morales Olazábal, *Safe Harbor for Forward-Looking Statements Under the Private Securities Litigation Reform Act of 1995: What's Safe and What's Not?*, 105 DICK. L. REV. 1, 3 (2000).

[193] Security researchers have experienced frequent threats of litigation. *See* SUNOO PARK & KENDRA ALBERT, A RESEARCHER'S GUIDE TO SOME LEGAL RISKS OF SECURITY RESEARCH 3 (2020), https://clinic.cyber.harvard.edu/wp-content/uploads/2020/10/Security_Researchers_Guide-2.pdf [https://perma.cc/HRD7-J4NZ]; *see also* Zack Whittaker, *Lawsuits Threaten Infosec Research — Just When We Need it Most*, ZDNET (Feb. 19, 2018), https://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/ [https://perma.cc/F927-UBB5] ("In other words, hackers and security researchers on the right side of the law are more likely to self-censor if they think they may be sued, or others are successfully sued—for doing their jobs.").

the Department of Justice framework and not bring civil suits against the researchers, or to initiate a complaint to law enforcement.[194]

The Cybersecurity Information Sharing Act of 2015 also contains a safe harbor provision.[195] In order to encourage the private sector to share cybersecurity information with the federal government (such as the fact that a company had been hacked, for example), the safe harbor provision offers a shield from civil, regulatory, and antitrust liability.[196]

Other examples of technology safe harbors include state government data breach notification laws. Almost all states have laws requiring companies to report certain data breaches, but recently some states are now adding safe harbor provisions to these laws.[197] The provisions encourage companies to

[194] U.S. DEP'T JUST., A FRAMEWORK FOR A VULNERABILITY DISCLOSURE PROGRAM FOR ONLINE SYSTEMS 7 (2017), https://www.justice.gov/criminal-ccips/page/file/983996/download#page=7 [https://perma.cc/P5J6-HKM2] (recommending specific language for organizations to adopt in their own policies for vulnerability disclosure can be found in Section III, Step 3, Item D of the framework: "Explain the consequences of complying—and not complying—with the policy"). In September 2020, the U.S. Cybersecurity and Infrastructure Security Agency ("CISA") issued Binding Operational Directive 20-01 requiring all federal departments and agencies to have a vulnerability disclosure policy and encouraging them to adopt DOJ language in their policy. *See* CYBERSECURITY & INFRASTRUCTURE AGENCY, BOD 20-01: DEVELOP AND PUBLISH A VULNERABILITY DISCLOSURE POLICY (2020), https://www.cisa.gov/news-events/directives/bod-20-01-develop-and-publish-vulnerability-disclosure-policy [https://perma.cc/367B-YAAK].

[195] *See* 6 U.S.C. § 1505; *see also* John Evangelakos, Brent J. McIntosh, Jennifer L. Sutton, Corey Omer & Laura S. Duncan, *Sullivan & Cromwell Discusses The Cybersecurity Act of 2015*, THE CLS BLUE SKY BLOG (Jan. 6, 2016), https://clsbluesky.law.columbia.edu/2016/01/06/sullivan-cromwell-discusses-the-cybersecurity-act-of-2015/ [https://perma.cc/S76Y-KFQH].

[196] *See* Evangelakos, McIntosh, Sutton, Omer & Duncan, *supra* note 195 ("Once triggered, [the Cybersecurity Information Sharing Act's] safe harbors from liability are broad. Private entities sharing information are generally shielded from civil, regulatory, and antitrust liability based on their sharing."); *id.* (noting later that the Cybersecurity Information Sharing Act also "does not expressly exclude instances of either gross negligence or willful misconduct from its liability protections," further emphasizing the broad nature of the safe harbor to encourage cybersecurity information sharing behaviors).

[197] Kayne McGladrey, *Three US State Laws are Providing Safe Harbor Against Breaches*, CYBER SEC. HUB (Sept. 8, 2021), https://www.cshub.com/security-strategy/articles/three-us-state-laws-are-providing-safe-harbor-against-breaches [https://perma.cc/8FRC-45DM] (explaining that the adoption of recommended cybersecurity frameworks, such as NIST SP 800-53, by private sector companies has been "haphazard," and that lawmakers are trying different approaches to improve the adoption of frameworks for cyber defenses by using legal safe harbor provisions). The three states that have enacted a safe harbor law for cybersecurity into legislation are Ohio in 2018, Utah in 2021, and Connecticut in 2021. *Id.*

adopt cybersecurity frameworks and invest more heavily in cybersecurity practices to prevent breaches before the damage occurs.[198]

B. Important Features of an Effective Blockchain Safe Harbor

The preceding examples make clear that safe harbor provisions can often help to shape the kind of responsible corporate and personal behavior that legislators hope to incentivize. Of course, the devil is in the details when it comes to such legislation. Precisely what a blockchain safe harbor provision should look like is beyond the scope of this Article. Whatever the ultimate form, it is crucial that any safe harbor provision that attempts to regulate blockchain take into consideration the lessons we have learned in the years since implementation of Section 230 and Section 512. Section 230 and Section 512 have some similar features and some key differences, as discussed above.[199] And the technological advance they were designed to protect—internet as we know it—is different in many respects from blockchain. And yet, the preceding Parts make clear that there are still key principles we can glean from the last twenty-five years about certain features that help improve or reduce a safe harbor provision's efficacy. These features include sunset provisions to be sure that the safe harbors are the right fit for evolving technology, language that is specific enough to provide guidance to courts and litigants but not so rigid as to become technologically obsolete, and a careful weighing of the pros and cons of industry involvement in the safe harbor legislative drafting process. Finally, an important feature that both Section 512 and Section 230 contain is a clear carve out for criminal, fraudulent behavior, and this will be especially important for any safe harbor that covers cryptocurrencies.

i. Sunset Provisions

As noted above, Section 230 has been increasingly criticized over the years. For example, its broad scope of protection has been criticized for creating too little incentive for social media platforms to remove disinformation from their sites.[200] Of course, social media did not exist at the time that Section 230 was passed, and so it would have been difficult to predict the impact of the law on

[198] *Id.*

[199] *See supra* Sections II.A–B.

[200] Ashley Johnson & Daniel Castro, *Fact-Checking the Critiques of Section 230: What Are the Real Problems?*, INFO. TECH. & INNOVATION FOUND. (Feb. 22, 2021), https://itif.org/publications/2021/02/22/fact-checking-critiques-section-230-what-are-real-problems/ [https://perma.cc/ALT9-UJ2C].

it. But it is not difficult to predict today that blockchain applications will almost certainly change and develop in ways that are hard to imagine at present. It is a basic truism of technology that it will evolve more quickly each year—and sometimes advance in unforeseen ways. For example, "Moore's Law," named after Intel co-founder George Moore, posits that computer processing power will double at a rate of roughly every one and a half years.[201] We know technology will advance at exponential rates, and thus the need for any technology regulation, including any safe harbor provision, to be regularly revisited and updated. What seemed like a good idea in 2022 might be hopelessly inadequate in 2042, or even a glaringly bad idea.

There are several ways this can be accomplished, including by requiring that the law be regularly reauthorized by Congress. "Sunset clauses deal with the problem of laws that linger even when the needs of the time no longer require them."[202] There is recent precedent for an aggressive use of sunset provisions from the Department of Health and Human Services (HHS), though the initiative ultimately failed. At the end of the Trump Administration, the HHS issued a final rule that "would have required the agency to examine most of its rules every decade, determine whether each regulation is 'significant' to small businesses and other small entities, and conduct a review of any significant regulation to determine whether it is still needed."[203] If the agency failed to complete this assessment in a timely manner, regulations would automatically "sunset" or expire.[204] Despite being lauded as a move that "will increase agency accountability and ensure that outdated HHS regulations do not

[201] Adam Thierer, *Sunsetting Technology Regulation: Applying Moore's Law to Washington*, FORBES (Mar. 25, 2012, 12:56 PM), https://www.forbes.com/sites/adamthierer/2012/03/25/sunsetting-technology-regulation-applying-moores-law-to-washington/?sh=19c431b55010 [https://perma.cc/FX3P-7C9Q].

[202] Mary D. Fan, *Privacy, Public Disclosure, Police Body Cameras: Policy Splits*, 68 ALA. L. REV. 395, 436 (2016); *see also* Jacob E. Gersen, *Temporary Legislation*, 74 U. CHI. L. REV. 247, 298 (2007) (discussing the history, advantages, and disadvantages of sunset provisions and other forms of temporary legislation and concluding: "Normatively, temporary legislation should not be globally eschewed, and at least in specific policy domains such as responses to newly recognized risk, there should be a presumptive preference in favor of temporary legislation").

[203] Martin Totaro & Connor Raso, *Agencies Should Plan Now for Future Efforts to Automatically Sunset Their Rules*, BROOKINGS INST. (Feb. 25, 2021), https://www.brookings.edu/research/agencies-should-plan-now-for-future-efforts-to-automatically-sunset-their-rules/ [https://perma.cc/8UBS-Y5TS].

[204] *Id.* ("Significant regulations would have automatically expired (or 'sunsetted') if the agency did not assess and, where required, review the rules by the deadline.").

unnecessarily burden the American public through sheer inertia,"[205] the agency ultimately withdrew the rule.[206] But the HHS has included sunset provisions on safe harbor provisions in connection with physician anti-kickback laws, reasoning that such provisions are a "partial check" against the danger that the safe harbors will be abused.[207]

Having sunset provisions in any regulation would require Congress to revisit them in light of any changed circumstances (or even in light of any perceived judicial "misinterpretation"). A sunset provision, or even a time-limited grace provision such as the one proposed by SEC Commissioner Peirce,[208] can help make sure the safe harbor does not outlive its usefulness. One commentator has even proposed applying Moore's Law directly to technology regulations, arguing that "[e]very new technology proposal should include a provision sunsetting the law or regulation 18 months after enactment."[209] Although such an aggressive timeline may be unnecessary, automatically ending safe harbors after three to five years would force Congress to assess their impact. If the determination is that the safe harbor provision is functional and beneficial, it can always be reauthorized. If it has grown beyond what Congress initially intended, either because of technological advances, unforeseen circumstances, or even judicial enlargement, it can be ended without any effort.

ii. The Safe Harbor Contours Must "Thread the Needle"

As discussed above, courts have generally construed the safe harbor provision found in Section 230 quite broadly.[210] This makes sense, given that the provision was written broadly and there were few "hurdles" service providers would need to clear in order to be eligible. By contrast, courts have

[205] Charles Yates, *The SUNSET Provision for Old Regulations Will Improve Agency Accountability*, HILL (Feb. 22, 2021, 8:30 AM), https://thehill.com/opinion/finance/539507-the-sunset-provision-for-old-regulations-will-improve-agency-accountability/ [https://perma.cc/4X5D-EMLN].

[206] Withdrawing Rule on Securing Updated and Necessary Statutory Evaluations Timely, 87 Fed. Reg. 32,246 (May 27, 2022).

[207] John W. Hill, Arlen W. Langvardt & Anne P. Massey, *Law, Information Technology, and Medical Errors: Toward a National Healthcare Information Network Approach to Improving Patient Care and Reducing Malpractice Costs*, 2007 U. ILL. J. L. TECH. & POL'Y 159, 223 ("HHS envisioned the sunset provision as a partial check against the potential danger that the safe harbor might be abused, given the considerable economic value of the items and services involved.").

[208] *See* Peirce, *supra* note 185.

[209] Thierer, *supra* note 201.

[210] *See supra* Section II.A.2.

at times construed the DMCA Section 512 safe harbor provisions broadly and at other times have read more narrowly the requirements, such as requiring that copyright holders consider fair use before sending a takedown notice.[211] This too makes sense, because Section 512 of the DMCA requires some effort by service providers before they are eligible for the safe harbor—they have to promptly remove infringing material upon receiving proper notice, have to promptly notify the person who posted the allegedly infringing material, and have to promptly reinstate the material if they receive a proper counternotification, for example. Thus, there is arguably less risk that a safe harbor that requires some affirmative action on the part of the person or entity seeking protection will grow significantly beyond the bounds that Congress initially intended and immunize significantly more behavior that was never intended to be protected. This is because there is less risk that judges will construe the provisions more broadly than they were intended.

As policymakers consider a safe harbor of some kind for blockchain, they should be mindful of these examples. When courts are left to "gap fill" for a silent or ambiguous statute, they rely on certain canons of statutory construction. They are, for example, to assume that words have their ordinary meaning. For judges confronted with an ambiguous safe harbor provision, it is to be expected that they will read the text broadly and in favor of potential defendants given the presumed intent to provide protection for those very defendants.[212] After all, a safe harbor provision is just that: a manifestation of Congress's intent to protect a specified class of defendants from potential regulatory or private actions. There are many examples of courts construing the safe harbor provisions of a variety of other laws broadly,[213] even when there is reason to think congressional intent was that the provision be construed more

[211] *See* ZITTRAIN, *supra* note 4, at 119.

[212] In some ways, this is similar to the rule of lenity in criminal law. The rule of lenity is "a rule of statutory construction that requires a court to resolve statutory ambiguity in favor of a criminal defendant, or to strictly construe the statute against the state." David S. Romantz, *Reconstructing the Rule of Lenity*, 40 CARDOZO L. REV. 523, 524 (2018).

[213] *See, e.g.*, Brian D. Coggio, *The Scope of the "Safe Harbor" Provision of the Hatch-Waxman Act in View of* Merck v. Integra Lifesciences, 16 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1, 10 (2005) ("With minor exceptions, the courts have adopted an expansive reading of the [Hatch-Waxman Act] safe harbor exemption.").

narrowly.[214] Courts are especially likely to construe a safe harbor provision broadly when it is a criminal law at issue.[215]

Thus, where a safe harbor provision is relatively sparse, and requires little on behalf of those who would invoke it, it will be more likely to be read broadly. Where Section 230 requires relatively little, only that defendants be internet service providers and not be violating criminal law, courts read the protection broadly, even as technology changes to include applications never considered by Congress in passing the law. Where the DMCA Section 512 requires somewhat more, and puts affirmative obligations on defendants to do things like promptly take down material they have been informed is infringing, courts read those sections more strictly.

Therefore, if Congress enacts a blockchain safe harbor provision that is uncertain, it is more likely that courts will read it broadly, perhaps more broadly than Congress ever intended. And there are other problematic outcomes from uncertainty in a safe harbor provision, including that it is unlikely to produce the kinds of benefits Congress intended in enacting it. As two scholars noted in discussing the Section 512 safe harbor, "[u]ncertainty comes at a cost, especially when safe harbors are concerned. First, an unclear safe harbor is largely self-defeating; safe harbors, by their very nature, are supposed to provide actors with certainty."[216]

Of course, lawmakers who enact a safe harbor provision for blockchain or any technology have to thread a needle: the provision must be certain enough to not produce unintended consequences or judicial enlargement, but also

[214] *See* Rachel Schneller Ziegler, *Safe, But Not Sound: Limiting Safe Harbor Immunity for Health and Disability Insurers and Self-Insured Employers Under the Americans with Disabilities Act*, 101 MICH. L. REV. 840, 848 (2002) (arguing that the "language of the [Americans with Disabilities Act], its legislative history, and agency interpretations, as well as other health care safe harbors, support a limited interpretation of the reach of the safe harbor provision," but nonetheless concluding that "despite Congress's intent, courts have interpreted the provision broadly, such that insurers and employers are nearly immunized from the requirements of the ADA").

[215] Elizabeth Sebesky, *More than Advisory: How Courts and the Justice Department Can Work Together to Fill Gaps in the Foreign Corrupt Practices Act*, 53 AM. CRIM. L. REV. 479, 502 (2016) ("'[S]afe harbors' to a criminal offense are to be construed broadly in favor of the defendant.").

[216] Lital Helman & Gideon Parchomovsky, *The Best Available Technology Standard*, 111 COLUM. L. REV. 1194, 1207 (2011). Helman and Parchomovsky argue that uncertainty in a safe harbor provision can also overly incentivize risk aversion and incentivize strike suits. *Id.* at 1207–08; *see also* Avery Minor, Note, *Cryptocurrency Regulations Wanted: Iterative, Flexible, and Pro-Competitive Preferred*, 61 B.C. L. REV. 1149, 1173 (2020) ("At best, critics argue, an ambiguous safe harbor is not useful because it provides no guidance for liability avoidance and, at worst, it can act as a false promise of immunity.").

flexible enough to not be technically obsolete almost immediately upon passage. Despite acknowledging the criticisms of the Section 512 safe harbor provisions, one scholar nonetheless concludes that "statutory vagueness allows the safe harbors to remain applicable in a radically different technological era."[217] Lawmakers will have to tread lightly in order to produce a blockchain safe harbor that does more good than harm.

iii. Need to Balance Industry Involvement

It is not unusual for there to be industry involvement in the development of legislation, even if this practice is not often discussed openly by lawmakers.[218] For example, there is a well-documented history of the Walt Disney Company aggressively lobbying for certain copyright laws, and Disney issues many DMCA take down notices each year.[219] But the history of early internet regulation makes clear that industry involvement in developing any safe harbor regulation needs to be balanced and tempered, and also that the large companies who currently lead the industry should not be the only "industry" consulted.[220]

There is, of course, a documented history of industry involvement in internet regulation; recall from the discussion above on the history of Section 230 that lawyers for America Online and Prodigy were involved in its development.[221] As one scholar noted, American technology companies are "repeat players" in the legislative process, and "[t]hey spend millions lobbying the government on a whole range of issues—for instance, one analysis found

[217] Minor, *supra* note 216, at 1173. Minor also argues that "[b]ecause the safe harbors contain broad language but encompass a specific set of ISP conduct, they have remained applicable to ISPs today even though twenty years have passed since the inception of the DMCA." *Id.* at 1180.

[218] *See, e.g.*, Ganesh Sitaraman, *The Origins of Legislation*, 91 NOTRE DAME L. REV. 79, 106 (2015) ("Legislative drafts can also emerge from private authors—interest groups, industry, academics, individual policy experts, or bodies of experts like the Administrative Conference or the American Law Institute. In these cases, the draft is passed through to [members of Congress's] office, and the [member of Congress]adopts the draft as her own. The practice is frequent, though examples tend not to be public because [members of Congress] do not want to concede they let interest groups draft their legislation.").

[219] *See, e.g.*, Stacey M. Lantagne, *Building a Better Mousetrap: Blocking Disney's Imperial Copyright Strategies*, 12 HARV. J. SPORTS & ENT. L. 141, 156 (2021) (describing Disney's "tactics of enforcing its intellectual property through legislative lobbying, aggressive litigation, strategic trademarking, and other anti-competitive acts," and its use of DMCA takedown notices).

[220] *Id.*

[221] KOSSEFF, *supra* note 27, at 61 (noting that Representatives Cox and Wyden "met with a small group of like-minded advocates," including a lawyer for Prodigy and a lawyer for America Online, when they were drafting the language that eventually became Section 230).

that major tech players lobby the government on as many as a hundred issues a year."[222]

Although industry involvement in regulation is nothing new and is not inherently "bad," there is a real risk to users when industry gets too large a seat at the table. Further, when only large industry players have the ability to lobby, there is a risk that the law will be drafted in a way that advantages current industry leaders and excludes smaller start-ups.[223] Thus, advocates have, for example, urged against further rewriting the DMCA in light of the experiences of large tech companies like Facebook and YouTube.[224]

As lawmakers consider blockchain regulations, and especially any blockchain safe harbor provisions, it is natural that there will be some communication with industry lobbyists, and notably the large technology companies who have the most resources to lobby. But it is also crucial that legislators bear in mind that those companies will have incentives to push for legislation that protects their already-dominant market position.[225] Yesterday's scrappy start-up company is today's powerful industry, or, as Jonathan Zittrain put it, "the barbarians of yesterday have themselves become the gatekeepers of today."[226] Any blockchain safe harbor should be carefully considered in light

[222] *Standing, Surveillance, and Technology Companies*, 131 HARV. L. REV. 1742, 1757 (2018).

[223] *See* Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CALIF. L. REV. 1221, 1262 (2022) ("Dominant companies also have more influence over regulators and regulations. . . . Plus, representatives from the most powerful technology companies have been the most common invitees at congressional hearings on privacy. And, given the revolving door between government service and lucrative positions representing technology companies, regulators have a serious incentive to develop stronger relationships with companies like Facebook and Google than with their far smaller competitors."); *see also* Cyphert & Martin, *supra* note 37, at 202 (citing Matt Perault, *Well-Intentioned Section 230 Reform Could Entrench the Power of Big Tech*, SLATE (June 1, 2021, 9:00 AM), https://slate.com/technology/2021/06/section-230-reform-antitrust-big-tech-consolidation.html [https://perma.cc/J8U8-DBZG]); *see also* Tate Ryan-Mosley, *How the Supreme Court Ruling on Section 230 Could End Reddit as We Know it*, MIT TECH. REV. (Feb. 1, 2023), https://www.technologyreview.com/2023/02/01/1067520/supreme-court-section-230-gonzalez-reddit/ [https://perma.cc/TL5E-F9LZ] (discussing the fear that Section 230's liability shield "will leave smaller technology companies unable to compete with the bigger companies that can afford to fight a host of lawsuits," and noting "that Section 230 protects smaller internet companies that don't have large litigation budgets").

[224] *See* Trendacosta, *supra* note 100 ("Almost everything you use online relies in some way on the safe harbor provided by section 512 of the DMCA. Restructuring the DMCA around the experiences of the largest players like YouTube and Facebook will hurt users, many of which would like more options rather than fewer.").

[225] As another scholar puts it, "what is good for a monopolist is not usually good for society." Waldman, *supra* note 223, at 1263.

[226] Zittrain, *supra* note 2, at 142.

of not only the interests of industry, but also of those who invest in applications like cryptocurrencies, especially in light of documented instances of fraud and abuse in that sector.

iv. Avoid Providing a Safe Harbor for Fraudulent Behavior

Blockchain, and specifically cryptocurrencies, offer privacy and pseudonymity. As discussed above, these features can be very attractive to cyberlibertarians.[227] Unfortunately, they can also be quite attractive to people who wish to engage in overtly criminal behavior, including illegal drug trafficking and even human trafficking.[228]

Beyond their use to fund illegal activity, cryptocurrencies have also been shaken in recent years by allegations of massive frauds, including some charged by criminal prosecutors, as well as allegations of market manipulation. One recent study concluded that more than three quarters of the initial coin offerings (ICOs) offered in 2017 were "scams."[229] The Federal Trade Commission recently warned the public that "[c]ryptocurrency scams are now a popular way for scammers to trick people into sending money."[230] SEC Commissioner Crenshaw, in speaking out against Commissioner Peirce's safe harbor proposal, said that she worried about "relaxing regulatory requirements in markets prone to investor protection failures, [and] limited investor redress options because of pseudonymity . . . disintermediation, and market manipulation."[231] Whatever

[227] *See supra* Section III.A.2.

[228] *See generally* ANDY GREENBERG, TRACERS IN THE DARK: THE GLOBAL HUNT FOR THE CRIME LORDS OF CRYPTOCURRENCY (2022) (describing law enforcement's efforts to crack down on the use of cryptocurrencies to fund illegal activities, including human trafficking); Jane Khodarkovsky, April N. Russo & Lauren E. Britsch, *Prosecuting Sex Trafficking Cases in the Wake of the Backpage Takedown and the World of Cryptocurrency*, 69 DEP'T JUST. J. FED. L. & PRAC. 101, 119 (2021) ("Because human trafficking is so lucrative and often requires moving around large amounts of money, cryptocurrency is increasingly used to facilitate it."); Nicholas J. Ajello, *Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination*, 80 BROOK. L. REV. 435, 442 (2015) ("The anonymous, near-untraceable nature of Bitcoin has undoubtedly attracted criminals to the currency.").

[229] Neitz, *supra* note 143, at 189 ("One study reported that approximately 78 percent of the ICOs offered in 2017 were actually scams.").

[230] Cristina Miranda, *Avoiding a Cryptocurrency Scam*, FED. TRADE COMM'N (July 16, 2020), https://www.consumer.ftc.gov/blog/2020/07/avoiding-cryptocurrency-scam [https://perma.cc/QKU9-FKGK].

[231] Crenshaw, *supra* note 186.

else a safe harbor provision does, it is essential that it not inadvertently protect, incentivize, or reward fraudulent behavior.[232]

Section 230 explicitly carves criminal behavior out from its safe harbor provision, providing only protection against civil liability.[233] Congress even clarified in 2018 that Section 230 has "no effect on sex trafficking law."[234] Section 512 likewise provides only immunity from liability for "monetary relief, or . . . for injunctive or other equitable relief."[235] Any blockchain safe harbor provision should be similarly limited to immunity from civil suit. If lawmakers choose to immunize actors against criminal action (such as a criminal Securities Enforcement Commission action), they should have a very compelling reason to do so and should write the safe harbor in as limited a fashion as is possible.

V. CONCLUSION

"Cyber-libertarianism remains a beautiful dream. But the idea that all online communities will successfully enforce their own rules, without regard for governments, will fare as poorly as it did the first time. It already has."[236] Blockchain systems will face additional regulation, and that regulation is coming quickly. There are already legislative safe harbor provisions pending before Congress.[237] There is good reason to believe that one or more safe harbor provisions will ultimately be enacted for blockchain applications. The lessons of early internet regulation demonstrate that such safe harbors, while perhaps

[232] Strange though it may seem, there *are* times that lawmakers have chosen to provide safe harbors to behavior that would otherwise be fraudulent. For example, there are multiple safe harbors that exist to the fraud and abuse laws that surround healthcare spending regulation. *See* Soraya Ghebleh, *No VIP Treatment: ACOs Should Not Get Waiver Protection from the Prohibition on Beneficiary Inducement*, 70 VAND. L. REV. 737, 753 (2017) ("Safe harbor regulations were introduced in order to protect specific business practices that would not be deemed unlawful or contrary to the statutory intent of the healthcare fraud laws but that could easily be textually interpreted to be in violation of these laws.").

[233] "Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of Title 18, or any other Federal criminal statute." 47 U.S.C. § 230(e)(1).

[234] *Id.* § 230(e)(5). The amendment, entitled "Allow States and Victims to Fight Online Sex Trafficking Act of 2017" clarified that Section 230 "was never intended to provide legal protection to websites that unlawfully promote and facilitate prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims." Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (2018).

[235] 17 U.S.C. § 512(a).

[236] Werbach, *supra* note 10, at 492.

[237] *See* Peirce, *supra* note 185.

essential for technological growth and adoption, can have unintended consequences. By being mindful of the lessons learned from the implementation of Section 230 and Section 512, regulators can hope to avoid some of these unintended consequences. Regulation is necessary, but it does not have to destroy entirely the philosophical goals of the early blockchain enthusiasts. If we learn from the history of internet regulation, perhaps this new era of blockchain regulation can be, in the words of John Perry Barlow, more "humane and fair" than that which came before.[238]

[238] Barlow, *supra* note 1 ("We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.").