

11-2024

Trustless Trust and Antitrust: A Synthesis

Matt Blaszczyk

University of Michigan School of Law

Follow this and additional works at: <https://digitalcommons.tourolaw.edu/lawreview>



Part of the [Antitrust and Trade Regulation Commons](#)

Recommended Citation

Blaszczyk, Matt (2024) "Trustless Trust and Antitrust: A Synthesis," *Touro Law Review*. Vol. 39: No. 4, Article 3.

Available at: <https://digitalcommons.tourolaw.edu/lawreview/vol39/iss4/3>

This Article is brought to you for free and open access by Digital Commons @ Touro Law Center. It has been accepted for inclusion in Touro Law Review by an authorized editor of Digital Commons @ Touro Law Center. For more information, please contact lross@tourolaw.edu.

TRUSTLESS TRUST AND ANTITRUST: A SYNTHESIS

*Matt Blaszczyk**

ABSTRACT

Authors have written of antitrust law's demise in the face of blockchain, which, seemingly, achieves the pro-competitive ends of the law through technology and private ordering. Permissionless blockchains in particular are said to offer a vision of radical disintermediation and a break with the platform economy troubling the regulators today. At the same time, blockchain supposedly presents challenges to antitrust doctrine, from the most basic of concepts to the viability of enforcement and remedies. Finally, blockchain community governance is said to allow for private ordering of antitrust, i.e., enforcement of rules attempting to protect competition, which are at the same time illegal; not coming from the courts or agencies, they constitute competition wrongs themselves.

This Article argues that all three claims are overstated and proposes a synthesis of law and code. The legal doctrine can be modified to tackle the novel technological landscape quite easily, with adoption of novel legal fictions. This is necessary since blockchains—both public and even more so private ones—while ingenious, do not remove a need for the law to protect the market from anticompetitive conduct. Indeed, even public ledgers have power structures allowing for abuse, while private blockchains may, in fact, allow for its proliferation. The law needs to find a regulatory access point to the ledgers. This is not an easy task; however, cooperation of blockchains with the law, and encoding of antitrust rules on the ledgers themselves, offers a possibility of a reconciliation between the law and the code. At the same time, this lends legitimacy to pro-competitive actions of those cyberspace

* Research Fellow in the Law and Mobility Program, University of Michigan Law School; LL.M., Georgetown University Law Center; LL.B., Dickson Poon School of Law, King's College London; Center for Transnational Legal Studies, London. I am grateful to Professor John D. Graubert for his guidance and support.

communities and ensures a preservation of the rule of law. This is the blockchain antitrust synthesis.

I. INTRODUCTION

Scholars have long recognized that technology is a regulatory force, with rules “crafted by extra-legal players in extra-legal institutions,”¹ and that private ordering and the code itself are modalities with which private law needs to interact.² In other words, the technological infrastructure—ordering through contract, license, and computer code employed by the market players—factually regulates much of social life, which was traditionally governed by state law.³ At the same time, scholars emphasize that not only does technology and its novel use-cases co-regulate but also may undermine existing legal legacy solutions, such as the established organizational forms and legal doctrines.⁴ The technological specifications of blockchain—decentralization, immutability and automatic execution, and pseudonymity⁵—together

¹ Margot E. Kaminski, *Technological “Disruption” of the Law’s Imagined Scene: Some Lessons from Lex Informatica*, 36 BERKELEY TECH. L.J. 883, 884 (2022) (cleaned up).

² See generally LAWRENCE LESSIG, CODE VERSION 2.0 (2006).

³ See generally *id.*; MARGARET JANE RADIN, BOILERPLATE (2013). I explored these issues in detail insofar as they relate to blockchains and smart contracts elsewhere. See Matt Blaszczyk, *Blockchain and Private Law* (Jan. 6, 2023), <https://ssrn.com/abstract=4319649>; Matt Blaszczyk, *Smart Contracts, Lex Cryptographia, and Transnational Contract Theory* (Feb. 13, 2023), <https://ssrn.com/abstract=4319654>.

⁴ Julie E. Cohen, *From Lex Informatica to the Control Revolution*, 36 BERKELEY TECH. L.J. 1017, 1020 (2022) (arguing that code is not just a mode of regulation but a “mode of development that catalyzes deep structural transformation in organizations of all sorts, including the organizational forms of legal institutions carefully stewarded – and venerated – over decades and centuries”). See generally LESSIG, *supra* note 2; see also RADIN, *supra* note 3 (showing how code replaces the law of contract); see generally Margaret Jane Radin, *Regime Change in Intellectual Property: Superseding the Law of the State with the “Law” of the Firm*, 1 U. OTTAWA L. & TECH. J. 173 (2004) (showing how code supersedes the law of copyright); Tim Wu, *When Code Isn’t Law*, 89 VA. L. REV. 679, 682 (2003) (applying Lessig insights to analyze the use of code as a means of avoiding copyright law).

⁵ As I explained elsewhere:

Permissionless blockchains are . . . pseudonymous, with parties not having to reveal their true identities to store information and transact, allowing for transactions between persons that do not know or trust each other. Pseudonymity makes it more difficult to determine who the users of a network are and who one is contracting with, since blockchain records addresses, not names. . . It is important to contrast the pseudonymity of the blockchain with anonymity. Since blockchains are public and decentralized, they

with institutional possibilities they offer, i.e., radical disintermediation and elimination of the need for *trust* from dealings between parties,⁶ operation of markets without centralized intermediaries, with low networking costs, have led some to argue that a *lex cryptographia* emerges.⁷ In the realm of competition, law scholars ask if the cryptographically generated “trustless trust”⁸ will lay a fatal blow to antitrust.⁹ In this spirit, Thibault Schrepel proclaimed: “Antitrust law as we know it must die and be reborn. If not, it soon will be illegitimate.”¹⁰

operate in a transparent manner and provide anyone with the ability to pinpoint each and every transaction that a given account has engaged in. Consequently, the entries on the ledger provide an audit trail and evidence of wrongdoing, which can be established given enough time and effort, and many parties to a transaction can be unmasked. One may use contextual information and probabilistic methods to deanonymize individuals and effectively anyone can follow the flow of digital currency transactions and assess the degree of ‘affiliation’ that every new digital currency transaction enjoys with another.

Blaszczyk, *Blockchain*, *supra* note 3, at 28-29 (footnotes and quotation marks omitted).

⁶ Cristina Poncibò & Larry A. DiMatteo, *Smart Contracts: Contractual and Non-contractual Remedies*, in THE CAMBRIDGE HANDBOOK OF SMART CONTRACTS, BLOCKCHAIN TECHNOLOGY AND DIGITAL PLATFORMS 118, 122-23 (Larry A. DiMatteo et al. eds., 2020) (hereinafter CAMBRIDGE HANDBOOK). The blockchain-enabled trustless trust means that it is “possible to trust the outputs of a system without trusting any actor within it.” *Id.* (footnotes and citations omitted). It is thus unnecessary to trust either an intermediary or a central authority such as the state—but merely the code itself.

⁷ See generally PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 5 (2018) (writing that with blockchains, people can create private regulatory frameworks without the need for the law of a sovereign state, fashioning an analogy to the medieval *lex mercatoria*).

⁸ See Primavera De Filippi et al., *Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance*, 62 TECH. IN SOC’Y 1, 25-26 (2020) (arguing that blockchain, rather than being trustless, is a distributed trust confidence machine, creating shared expectations regarding the manner of operation and its correctness. In this way, blockchain “produces confidence (and not trust) . . . based on an understanding of their procedural and rule-based functioning” thereby eliminating the need for any centralized “trusted” authority, as well as the requirement to trust any of the actors who interact over a blockchain network.”). *Id.*

⁹ See Thibault Schrepel, *Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox*, 3 GEO. L. TECH. REV. 281, 285 (2019).

¹⁰ *Id.* at 338.

Obviously, technological change influences how “policymakers and judges think about competitive markets and, consequently, antitrust rules.”¹¹ Although up until recently the debate about blockchain did not focus on antitrust issues,¹² the challenge that blockchain poses to competition law and policy has already been studied by the Organisation for Economic Co-operation and Development (OECD).¹³ In the United States, both the Department of Justice (DOJ) Antitrust Division¹⁴ and the Federal Trade Commission (FTC) have undertaken first steps in the area,¹⁵ though they have yet to provide any detailed guidance.¹⁶ The efforts may intensify because President Biden’s *Executive Order on Ensuring Responsible Development of Digital Assets* encouraged the Attorney General, the Chair of the FTC, and the Director of the Consumer Financial Protection Bureau (CFPB) to “consider what, if any, effects the growth of digital assets could have on competition policy.”¹⁷

This Article analyzes the now burgeoning blockchain and antitrust literature, together with the recent case-law, showing that

¹¹ Laura Phillips Sawyer, *US Antitrust Law and Policy in Historical Perspective*, 19-110 HARV. BUS. SCH. WORKING PAPER 1, 26 (2019).

¹² Konstantinos Stylianou, *What Can the First Blockchain Antitrust Case Teach Us About the Crypto-Economy?*, JOLT: DIGEST (Apr. 26, 2019), <https://jolt.law.harvard.edu/digest/what-can-the-first-blockchain-antitrust-case-teach-us-about-the-crypto-economy/> (“Of all the areas blockchain has made headlines in, antitrust has ranked fairly low.”).

¹³ See *Hearing on Blockchain and Competition Policy*, OECD (June 8, 2018), [https://one.oecd.org/document/DAF/COMP/WD\(2018\)47/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf) at 3.

¹⁴ Makan Delrahim, “*Never Break the Chain*”: *Pursuing Antifragility in Antitrust Enforcement*, Thirteenth Annual Conference on Innovation Economics Kellogg School of Management, NW. UNIV. 1, 12-13 (Aug. 27, 2020), <https://www.justice.gov/opa/speech/file/1310506/download> (“Our goal at the Division is to inquire how disruptive innovators might be deploying [blockchain] technologies and how incumbents might try to stop or co-opt them. There is also, most certainly, potential for abuse. Incumbents could use blockchains anticompetitively to exclude competition.”).

¹⁵ See generally Neil Chilson, *It’s Time for a FTC Blockchain Working Group*, Fed. Trade Comm’n (Mar. 16, 2018), <https://www.ftc.gov/news-events/blogs/tech-ftc/2018/03/its-time-ftc-blockchain-working-group>.

¹⁶ Evan Miller & Hill Wellford, *Executive Order Encourages Antitrust Enforcers to Consider the Effect of Cryptocurrency and Blockchain Technology on Competition Policy*, INSIGHT (Mar. 11, 2022), <https://www.velaw.com/insights/executive-order-encourages-antitrust-enforcers-to-consider-the-effect-of-cryptocurrency-and-blockchain-technology-on-competition-policy/>.

¹⁷ Exec. Order No. 14067, 87 Fed. Reg 14143 (Mar. 9, 2022).

permissionless blockchains (i.e., ones which are open and accessible to everyone, without a need for permission, revealing one's identity, or significant transaction costs, e.g., Bitcoin, Ethereum¹⁸) substantially achieve many ends of competition law. This is timely, since the promise of a disintermediated economy offered by blockchain comes at a time when cyberspace infrastructure, or the web 2.0, has become consolidated in supposedly monopolistic platforms.¹⁹ The third era of cyberspace evolution is hoped by some to bring about the demise of the big tech, i.e., an era of disintermediated internet based on permissionless, community driven blockchains, without a need for powerful, centralized private autocracies such as Meta or Twitter.²⁰ This vision of the Internet's future should be especially attractive to those worried about the platforms' power expanding "without limit through scale and scope economies and network effects."²¹

At the same time, blockchains, whether public or private, do not eliminate all competition law harms. Moreover, they present new challenges on the level of antitrust doctrine, which needs to be adapted to reach the novel technological-economic reality.²² Furthermore, even if the doctrinal analysis becomes nuanced enough to accommodate the new technology, there appear to be practical obstacles to enforcement, stemming from the technical difficulty of identifying the wrongdoers who are pseudonymous and from the immutability of the

¹⁸ DE FILIPPI & WRIGHT, *supra* note 7, at 31.

¹⁹ See Exec. Order No. 14036, 86 Fed. Reg 36987 (July 14, 2021) ("today a small number of dominant internet platforms use their power to exclude market entrants, to extract monopoly profits, and to gather intimate personal information that they can exploit for their own advantage."). See also Herbert Hovenkamp, *Antitrust and Platform Monopoly*, 130 YALE L.J. 1952 (2021).

²⁰ DE FILIPPI & WRIGHT, *supra* note 7, at 126 ("As blockchain technology further matures, [its] services could conceivably compete with intermediaries like Facebook, WeChat, Twitter, or Reddit, playing a greater role in shaping the way information, media, and communications are disseminated online and pushing aside existing rules aimed at preventing free speech and the dissemination of illicit content."). See also Alex Pazaitis et al., *Blockchain and Value Systems in the Sharing Economy: The Illustrative Case of Backfeed*, 125 TECH. FORECASTING & SOC. CHANGE 105, 105 (2017) (exploring blockchain potential in the sharing economy); Morshed Mannan & Nathan Schneider, *Exit to Community: Strategies for Multi-Stakeholder Ownership in the Platform Economy*, 5 GEO. L. TECH. REV. 1, 2 (2021) (same).

²¹ A. Douglas Melamed, *Antitrust Law and Its Critics*, 83 ANTITRUST L.J. 269, 269 (2020). See also Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 742-44 (2017).

²² See *infra* Part II.

blockchains, i.e., the fact that the self-executing infrastructural code and the transactions encoded thereon are very difficult to change.²³ Finally, and most interestingly, in antitrust and in other areas of the law alike, there emerges a mismatch between the blockchain reality and the law: blockchains attempt to achieve the aims of competition law through technological and market solutions.²⁴ Different ledgers are also likely to engage in private ordering of competition policy, i.e., community driven self-regulatory measures, which are likely to be considered violations of antitrust law, since they do not carry the legitimacy of legal measures.²⁵ In this way, private ordering through code is not only in tension with the neo-Brandeisian goal of embedding “social and collective values” in the structure of digital marketplaces.²⁶ It is also in tension with the basic rule of law principle that what happens on ledgers should not extend beyond the law’s reach.²⁷ Thus, we arrive at the blockchain antitrust paradox.²⁸

This Article argues that the law and blockchain can arrive at a synthesis. Part II considers and rejects the arguments (of the so-called *lex cryptographia* proponents) that competition law cannot or should

²³ See *infra* Part IV.

²⁴ See *infra* Part II.

²⁵ See *infra* Part III.

²⁶ Elettra Bietti, *Self-Regulating Platforms and Antitrust Justice*, 101 TEX. L. REV. 165, 165 (2022). According to Bietti, the Neo-Brandeisian imperative is to move beyond the formalist focus on “uniform and acontextual goals such as efficiency or total welfare maximization” and embrace the “republican ideals of economic and political equality: a wide dispersion of ownership, monopoly breakups, structural separation remedies, and democratic equality.” *Id.* at 199. Bietti argues that the reform of antitrust must be rooted in the “principles of political and relational equality in markets,” i.e., “cooperation, reciprocity, and collective empowerment.” *Id.* See generally TIM WU, *THE CURSE OF BIGNESS* (2018) (hereinafter WU, *CURSE*). Tim Wu proposes to replace the consumer welfare standard with a “protection of competition,” one founded on the values of “anti-monopoly, equality, and decentralized power.” *Id.* at 127-39. This stems from the tradition of “political antitrust,” which is concerned that “too much concentrated economic power will translate into too much political power, and thereby threaten the Constitutional structure.” *Id.* at 53-55. Wu relies on *Brown Shoe Co. v. United States*, 370 U.S. 294, 316 (1962) to write, that antitrust should protect from threats to “other values” such as “independence of smaller businesses or local control of industry.” *Id.* at 54.

²⁷ See Margaret Jane Radin, *The Rule of Law in the Information Age: Reconciling Private Rights and Public Values*, 4 J.L. PHIL. & CULTURE 83 (2009).

²⁸ See Schrepel, *supra* note 9, at 281-85.

not apply to blockchains as a matter of doctrine and antitrust theory.²⁹ Part III shows why the law should apply to the code, presenting the potential for monopolistic and collusive abuses on public and private ledgers, analyzing both the nature and use-cases of blockchains from the perspective of the U.S. and European Union (EU) law. There is potential for abuse but also for doctrinal remedy, and the theoretical impossibility claims are unwarranted. This has proven true in the cyberspace debate of decades prior but also, for example, at the time that *United States v. Microsoft*³⁰ was litigated, “commenters questioned whether antitrust could address the unique issues posed by the technology markets involved.”³¹ Yet, “the antitrust laws have proved adaptable to technological change in the computer and Internet eras, and that flexibility should continue in the blockchain era.”³² Reassuringly, it seems that most of the antitrust claims regarding blockchains are straightforward and that the technology can also be used to aid competition law and policy.³³

²⁹ See generally FILIPPI & WRIGHT, *supra* note 7, at 6, 126; KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST 102-04 (2018); Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L.J. 487, 492 (2018).

³⁰ 253 F.3d 34, 45-46 (D.C. Cir. 2001).

³¹ See *Competition in Digital Technology Markets: Examining Acquisitions of Nascent or Potential Competitors by Digital Platforms: Hearing Before the Subcomm. on Antitrust, Competition Pol’y, & Consumer Rts. of the S. Comm. on the Judiciary*, 116th Cong. 1 (2019) (statement of Bruce Hoffman, Dir. of the Bureau of Competition at the Fed. Trade Comm’n) (adding in footnote three that “[t]oday’s technology markets also pose highly unique challenges, and the Commission will endeavor to utilize our existing laws to protect American citizens and businesses from anticompetitive conduct.”).

³² Samuel N. Weinstein, *Blockchain Neutrality*, 55 GA. L. REV. 499, 542 (2021). See also, e.g., Andrew Finch, Principal Deputy Assistant Att’y Gen., Antitrust Div., U.S. Dep’t of Just., Address at Antitrust in the Financial Sector: Hot Issues & Global Perspectives (May 2, 2018) (“The agreement to fix the price is the illegal act; the means through which the agreement is carried out is less important.”). Cf. Herbert Hovenkamp, *Antitrust and the Movement of Technology*, 19 GEO. MASON L. REV. 1119, 1119 (2012) (“Determining the proper role of antitrust in high-technology markets is daunting . . .”).

³³ Weinstein, *supra* note 32, at 542. This essay does not discuss the blockchain in the context of mergers. This discussion has already been undertaken elsewhere. See THIBAUT SCHREPEL, BLOCKCHAIN+ANTITRUST: THE DECENTRALIZATION FORMULA 213-26 (2022); Jéssica Nemeth, *Blockchain, Behavioural Remedies, and Merger Control: How Can Access Remedies Do Better?*, 13 J. OF EUR. COMPETITION L. & PRAC. 167 (2022); Antoine Babinet & David Dubois, *‘Archipels’ Case: EU’s*

What does seem relatively novel is the potential for cyberspace communities to commit antitrust wrongs by trying to protect the competitive process and the practical obstacles to enforcement. This Article attempts to reconcile these two phenomena in Part IV. The law should incentivize blockchains to follow antitrust rules through various measures, thus incorporating itself into the code. At the same time, cooperation of blockchains with antitrust agencies and courts will lend legitimacy to those private ordering measures that protect the competitive process, ultimately solving the blockchain antitrust paradox.

II. THE PROMISE OF TRUSTLESS TRUST: TECHNOLOGY AS A SOLUTION TO COMPETITION PROBLEMS

“In the face of blockchain, current antitrust law may well be eliminated,”³⁴ wrote Schrepel. Fundamentally, much of competition law deals with trusts—a fiduciary relation in one sense, a “legal device used to coordinate multiple property owners through a unified management structure” in the other.³⁵ Blockchain, “widely seen as a new general-purpose technology,”³⁶ “eliminates the *need* for a fiduciary” through cryptography and automatic execution.³⁷ As Schrepel wrote, blockchain eliminates the “*raison d’être* of antitrust law, which will trigger epidermal reactions.”³⁸ In other words, blockchains eliminate top-down control thus increasing consumer welfare; however, commentators submit that antitrust cannot “impede blockchains’ development” in the process.³⁹ Blockchains thus create trust in the game theoretic sense, without employing the legal construct of a trust or a fiduciary relation.⁴⁰ This is the “blockchain antitrust paradox,” Schrepel claimed, arguing that if the technology provides a decentralized,

First Merger Control Analysis of a Private Blockchain Consortium, 12 J. OF EUR. COMPETITION L. & PRAC. 630 (2021).

³⁴ Schrepel, *supra* note 9, at 335 (cleaned up).

³⁵ Sawyer, *supra* note 11, at 2.

³⁶ Sinclair Davidson et al., *Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology* 1, 23 (July 19, 2016), <https://ssrn.com/abstract=2811995>.

³⁷ Schrepel, *supra* note 9, at 283.

³⁸ SCHREPEL, *supra* note 33, at 75 (sic).

³⁹ Thibault Schrepel & Vitalik Buterin, *Blockchain Code as Antitrust*, 2021 BERKELEY TECH. L.J. 1, 3 (2021).

⁴⁰ *Id.* at 4.

trustless process, the law is not only unnecessary but may become illegitimate; in any case, it will be impossible to enforce.⁴¹

This statement demands an instant qualification—it refers to permissionless blockchains, which are “public and . . . open to all [whereby] [t]he participant must have resources like computing power and software to validate transactions.”⁴² Put simply, “anyone in the network (nodes) can join the network and validate the blocks, anyone can read the chain and add new blocks to it.”⁴³ But there is another species—a private permissioned blockchain. These ledgers are akin to traditional databases, having institutional gatekeepers who can set rules and update the code easily.⁴⁴ The utopian dreams focus on the former, while the potential for abuse is greater on the latter. This Article tackles both.

A. Defining Trust

Exploring the “blockchain paradox” further, blockchains have been called “trust machines,”⁴⁵ supposedly generating “trustless trust,” i.e., making commercial activities trustworthy without the need to trust anyone in particular, be it an intermediary or a centralized power structure.⁴⁶ According to the proponents, rather than to trust intermediary institutions such as banks, courts, and governments, we can trust “math and computation, in the form of open-source cryptographic protocols.”⁴⁷ In other words, rather than trusting either the law or any party, users trust the immutable (i.e., supposedly unchangeable and self-executing) code, the cryptographically generated consensus mechanism,

⁴¹ Schrepel, *supra* note 9, at 336-37 (“Enforcing antitrust law amounts to imposing vertically designed rules and concepts on a technology built around the desire for decentralization.”). See also William Magnuson, *Regulating Fintech*, 71 VAND. L. REV. 1167, 1205 (“[D]ecentralization serves as a barrier to effective monitoring.”).

⁴² Toshendra Kumar Sharma, *Advantages and Disadvantages of Permissionless Blockchain*, BLOCKCHAIN COUNCIL (Oct. 4, 2018), www.blockchain-council.org/blockchain/advantages-and-disadvantages-of-permissionless-blockchain/.

⁴³ *Id.*

⁴⁴ Edmund Schuster, *Cloud Crypto Land*, 84 MOD. L. REV. 974, 975 (2021).

⁴⁵ See Chris Pike & Antonio Capobianco, *Antitrust and the Trust Machine*, OECD (2020), <http://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf> [<https://web-archival.org/2020-11-04/568616-antitrust-and-the-trust-machine-2020.pdf>].

⁴⁶ Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L.J. 487, 498 (2018).

⁴⁷ *Id.*

which is validated by all of the network's participants.⁴⁸ This is also where the pseudonymous nature of the code is important because while every user of a permissionless chain possesses a copy of all the transactions, the parties' real identities and what exactly is traded are unknown.

Despite the ingenuity of this solution, it should already become clear that trust is dependent on the code factually being unchangeable, which it may not be if the majority of users validating it decide to implement a change (also known as a *fork*).⁴⁹ Another difficulty is that, should a transaction on the chain be illegal (e.g., an unreasonable restraint of trade), it is both hard to detect and even harder to amend.⁵⁰ This in turn provokes another concern: are users trusting that the transactions are valid and unchangeable no matter their legal content, i.e., even if they are void by mistake or anticompetitive in character, or do they trust in only legally valid transactions? Moreover, while the architecture of decentralized networks generates some level of certainty that no abusive conduct will happen, this certainty is by no means absolute. This clash of the encoded and legal realities is a profound jurisprudential problem,⁵¹ which will undoubtedly affect competition law as well. Different kinds of failures of the technology undermine trust consumers place in it, while allowing for anticompetitive outcomes makes the case for legal intervention.⁵²

⁴⁸ See De Filippi et al., *supra* note 8, at 25-26 (Arguing that blockchain, rather than being trustless, is a distributed trust confidence machine, creating shared expectations regarding the manner of operation and its correctness. In this way, “[b]lockchain produces confidence (and not trust) . . . based on an understanding of their procedural and rule-based functioning . . . thereby eliminating the need for any centralized ‘trusted’ authority, as well as the requirement to trust any of the actors who interact over a blockchain network.”).

⁴⁹ Werbach, *supra* note 46, at 513 (“If someone controls more than half of the mining power in the network, they can validate blocks of their choosing, even if they involve double-spending.”). See *infra* Part III.

⁵⁰ See *infra* Part IV.

⁵¹ See generally Blaszczyk, *Smart Contracts*, *supra* note 3 (examining how smart contracts comply and deviate with jurisdictional requirements); Blaszczyk, *Blockchain and Private Law*, *supra* note 3 (undertaking a similar analysis for blockchain and private law at large).

⁵² See, e.g., Aaron Perzanowski, *How the Blockchain Undermined Digital Ownership*, 80 WASH. & LEE L. REV. 1137, 1153 (2023) (writing that “[t]echnological capabilities aside, the blockchain’s reputation as a reliable and trustworthy arbiter of transactions has taken a severe beating in recent years,” which makes legal intervention indispensable).

Trust in the competitive process is generated in part by the technology and free market, and while anticompetitive practices can still occur,⁵³ it is clear that there remains a need for antitrust law to become involved.⁵⁴ There is a historical observation that supports this point. The Sherman Act,⁵⁵ the first federal antitrust statute, was enacted at a time of economic and technological change; legislators ratified it when changes in transportation, production technology, finance, and business organization allowed individuals to do business more easily, at a bigger scale and without limiting geographical constraints.⁵⁶ Soon enough there emerged “trusts,” the popular name given to combinations of competitors who were able to affect consumer welfare by raising prices.⁵⁷ Together with innovation and new entity structures (such as the proto-holding companies, like Standard Oil), competition wrongs of cartelization and monopolization emerged.⁵⁸ This story repeated itself in cyberspace: beginning with a structurally decentralized and open web 1.0, we saw an emergence of big platforms of web 2.0, in a process Tim Wu called the “Cycle.”⁵⁹ The transformative potential of blockchain, with its new organizational (i.e., ledgers and organizations based on them) and transactional (smart contracts) means, signifies a return of the laissez-faire of the early days of competition law and the early days of cyberspace. As this Article

⁵³ See *infra* Part III.

⁵⁴ See *N. Pac. Ry. Co. v. United States*, 356 U.S. 1, 4–5 (1958) (alteration added):

The Sherman Act was designed to be a comprehensive charter of economic liberty aimed at preserving free and unfettered competition as the rule of trade. It rests on the premise that the unrestrained interaction of competitive forces will yield the best allocation of our economic resources, the lowest prices, the highest quality and the greatest material progress, while at the same time providing an environment conducive to the preservation of our democratic political and social institutions.... And to this end it prohibits [collusion and monopolization].

See also *United States v. Topco Assocs., Inc.*, 405 U.S. 596, 610 (1972) (“Antitrust laws...are the Magna Carta of free enterprise. They are as important to the preservation of economic freedom and our free-enterprise system as the Bill of Rights is to the protection of our fundamental personal freedoms.”).

⁵⁵ 15 U.S.C. §§ 1-2.

⁵⁶ Wayne D. Collins, *Trusts and the Origins of Antitrust Legislation*, 81 *FORDHAM L. REV.* 2279, 2281-82 (2013).

⁵⁷ *Id.* at 2280.

⁵⁸ *Id.* at 2292.

⁵⁹ TIM WU, *THE MASTER SWITCH* 10-13 (2010) (Wu defines the “Cycle” as an “oscillation of information industries between open and closed”; between laissez-faire, monopoly, and back again.).

explores in Part III, blockchains may nonetheless allow for competition wrongs to persist if not proliferate. In this way, the need for antitrust did not perish but remains, even if the headline-generating internet platforms will not survive the blockchain revolution.

B. Disintermediation of Internet Services

A *New York Times* article proclaimed that if blockchains succeed “their creations may challenge the hegemony of the tech giants far more effectively than any antitrust regulation.”⁶⁰ A recent economic study concluded that the “novel economic structure implied by Bitcoin’s innovative decentralized design ... protects users from monopoly pricing,” that “[c]ompetition among service providers within the platform and free entry imply no entity can profitably affect the level of fees paid by users.”⁶¹ Similarly effusive about the economic potential of blockchains, Pike and Carovano argue that permissionless blockchains offer “radical pro-competitive and inclusive efficiencies.”⁶² They claim that while a successful permissionless blockchain will have market power, they will be unable to exercise it.⁶³ In saying this, they rely on the classic belief that antitrust is supposed to protect decentralized processes, rather than outcomes.⁶⁴ However, as we will see in detail in Part III, centralization can occur, despite the nominally decentralized process through the employment of anticompetitive measures, but, of course, centralization can also occur innocently, through the operation of simple economic laws, to no detriment of

⁶⁰ Steven Johnson, *Beyond the Bitcoin Bubble*, N.Y. TIMES (Jan. 21, 2018, 11:41 AM), <https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html>.

⁶¹ Gur Huberman et al., *Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System*, 88 REV. OF ECON. STUD. 3011, 3011 (2021).

⁶² Chris Pike & Gabriele Carovano, *Reasons to be Cheerful: The Benevolent Market Power of Decentralised Blockchains*, in ALGORITHMIC ANTITRUST 107, 107 (Aurélien Portuese ed., 2022).

⁶³ *Id.* at 114-15 (They add that this is a perfect realization of “European competition law’s desire for an entity that exercises a special responsibility in its market dominance”) (cleaned up).

⁶⁴ SCHREPEL, *supra* note 33, at 69 (“Antitrust . . . prohibits centralization when it does not result from competition on the merits. But when it does, antitrust rules support centralized outcomes, as they increase consumer welfare by allowing them to benefit from better products and services.”); SchrepeL & Buterin, *supra* note 39, at 7 (arguing that both the EU and the U.S. competition law permits centralization when it results from competition on the merits, i.e., from a decentralized process).

consumers.⁶⁵ As we will note, too, centralized power structures have already emerged.⁶⁶ This may suggest that the resurrected trustbusting tradition of *United States v. Columbia Steel Co.*⁶⁷ and *Brown Shoe Co., Inc. v. United States*⁶⁸ embodying the vision of decentralized outcomes may not be content with the new technological reality, raising further need for enforcement, despite its practical difficulties.⁶⁹

Before assessing the anticompetitive dangers of the technology, we should address the claim that antitrust is wholly inapplicable to blockchains—a direct descendant of cyberlibertarian discourse from the beginning of web 1.0, notoriously unwelcoming of antitrust regulation.⁷⁰ Indeed, blockchain utopians make a twofold claim; on the one hand, they claim that blockchain will bring about a decentralized economy, without the platforms dominating today’s FTC struggles, and on the other, that they will be immune from regulation, whether as a matter of doctrine or practice.

⁶⁵ *Verizon Comm’ns Inc. v. Law Off. of Curtis V. Trinko*, 540 U.S. 398, 407 (2004) (“The mere possession of monopoly power, and the concomitant charging of monopoly prices, is not only not unlawful; it is an important element of the free-market system.”); Robert H. Bork & Ward S. Bowman, Jr., *The Crisis in Antitrust*, 65 COLUM. L. REV. 363, 368 (1965) (writing that centralization is linked to the “emerging efficiencies or economies of scale,” which benefits consumers, since “fewer of our available resources are being used to accomplish the same amount of production and distribution.”).

⁶⁶ See *infra* note 107.

⁶⁷ 334 U.S. 495, 536 (1948) (“Industrial power should be decentralized. It should be scattered into many hands so that the fortunes of the people will not be dependent on the whim or caprice, the political prejudices, the emotional stability of a few self-appointed men.”).

⁶⁸ 370 U.S. 294, 344 (1962) (“Congress appreciated that occasional higher costs and prices might result from the maintenance of fragmented industries and markets. It resolved these competing considerations in favor of decentralization. We must give effect to that decision.”).

⁶⁹ See Lina M. Khan, *The Ideological Roots of America’s Market Power Problem*, 127 YALE L.J.F. 960, 970-71 (2018) (Characterizing these cases as offering “drastically different descriptive and normative accounts of power,” to claim that the antitrust *ancien régime* “framework fails to adequately address market power [because] the law pegs liability to welfare *effects* rather than to the competitive *process*.”).

⁷⁰ See generally Daniel A. Crane, *Lochnerian Antitrust*, 1 N.Y.U. J.L. & LIBR. 496 (2005); DOMINICK T. ARMENTANO, *ANTITRUST: THE CASE FOR REPEAL* (2d ed. 2007); GARY HULL, *ABOLITION OF ANTITRUST* (2005).

C. Blockchains and Political Antitrust

The vision of the decentralized, deplatformed economy brought by permissionless blockchains superficially aligns well with the goals of competition law. The community driven web 3.0 paradigm seems to epitomize economic self-government, government of peers where the forces of the competitive process make the economic results fair, provided no abusive behavior occurs.⁷¹ If one were to be swayed by the techno-utopian narratives, blockchains are all like the idyllic Louisville of Justice Brandeis, a world of “economic democracy” free from “the curse of bigness.”⁷² If it were so, there would be no need for trust-busting or any governmental intervention, since the people and the market would solve all problems. In a sense, then, blockchain offers a promise that is radically democratic in the classical-liberal sense, distrusting and not needing the government.⁷³

At the same time, just like Louisville came to be corrupted by anti-democratic and anticompetitive processes, so in blockchains things can go wrong.⁷⁴ This is especially so on private, permissioned chains, where abuse may proliferate. Blockchains do not merely offer a return to the older conception of markets and democracy, however; they reinforce the *laissez-faire* through private ordering by code and immutable (i.e., practically unstoppable and unchangeable) smart contracts, which remove the market process from democratic control.⁷⁵ In this way, blockchain clashes outright with the neo-Brandeisian vision of both the market structure and competition law, which governs as inherently political,⁷⁶ and the demand to subject any “concentrated

⁷¹ See Eleanor M. Fox, *The Modernization of Antitrust: A New Equilibrium*, 66 CORNELL L. REV. 1140, 1154 (1981) (“The competition process is the preferred governor of markets. If the impersonal forces of competition, rather than public or private power, determine market behavior and outcomes, power is by definition dispersed, opportunities and incentives for firms without market power are increased, and the results are acceptable and fair.”) (citation removed).

⁷² See WU, CURSE, *supra* note 26, at 26.

⁷³ See WILLIAM MAGNUSON, BLOCKCHAIN DEMOCRACY: TECHNOLOGY, LAW AND THE RULE OF THE CROWD 5 (2020).

⁷⁴ *Id.* (“[M]arket forces may end up pushing even the most decentralized and democratic technologies in a centralized, antidemocratic direction.”).

⁷⁵ See Margaret Jane Radin, *The Deformation of Contract in the Information Society*, 37 OXFORD J. LEGAL STUD. 505 (2017).

⁷⁶ Zephyr Teachout & Lina Khan, *Market Structure and Political Law: A Taxonomy of Power*, 9 DUKE J. CONST. L. PUB. POL’Y 37, 37 (2014) (“Market structure is deeply political.”).

private power to democratic checks.”⁷⁷ The locus of control is in private hands rather than in those of the agencies or the political community at large.⁷⁸ While the notions of democracy and self-governance in antitrust remain elusive,⁷⁹ at the very least they demand a *possibility* of exercising structural interventions.⁸⁰ It should be clear that the tension is not just with the currently fashionable narrative of the value pluralist antitrust;⁸¹ blockchains, some claim, remove the markets from *any* governmental control, or more realistically, make said control more difficult.⁸² In this way, the utopian vision of blockchains is in tension with all schools of competition law, the belief in importance of antitrust for the preservation of the free market,⁸³ and the political philosophy of the last two hundred years.⁸⁴ Instead, a modification of the antitrust doctrine will allow for the law to reach blockchains and remedy competition wrongs which emerge on them.

⁷⁷ Tim Wu, *The Utah Statement: Reviving Antimonopoly Traditions for the Era of Big Tech*, MEDIUM (Nov. 18, 2019), <https://onezero.medium.com/the-utah-statement-reviving-antimonopoly-traditions-for-the-era-of-big-tech-e6be198012d7> (The inaugural statement of neo-Brandeisian scholars participating at the 2019 University of Utah conference, drafted by, among others, Tim Wu and Lina Khan); *see also* Lina Khan, *The New Brandeis Movement: America’s Antimonopoly Debate*, 9 J. EUR. COMPETITION L. & PRAC. 131, 131 (2018).

⁷⁸ *Cf.* Teachout & Khan, *supra* note 76, at 72 (“Decentralization of economic power in most areas of commerce is an essential underpinning of political freedom. . . . [Thus,] antitrust and other de-concentration rules should be understood not solely as part of corporate law, but also as part of political law.”) (alteration added).

⁷⁹ Daniel A. Crane, *Antitrust as an Instrument of Democracy*, 72 DUKE L.J. ONLINE 21, 22 (2022) (“if there is widespread agreement that antitrust law should serve as an instrument of democracy, there is little consensus on what that means or how it should happen.”).

⁸⁰ *Id.* at 29 (“Breaking the platforms’ ‘structural power’ entails structural antitrust interventions in service of democracy.”); *see also* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 498 (2019).

⁸¹ *See, e.g.,* Bietti, *supra* note 26; WU, CURSE, *supra* note 26; *see also* Ioannis Lianos, *Polycentric Competition Law*, 71 CURRENT LEGAL PROBLEMS 161 (2018).

⁸² *See* Usha R. Rodrigues, *Law and the Blockchain*, 104 IOWA L. REV. 679 (2019).

⁸³ *See* United States v. Topco Assoc., Inc., 405 U.S. 596, 610 (1972) (“Antitrust laws . . . are the Magna Carta of free enterprise. They are as important to the preservation of economic freedom and our free-enterprise system as the Bill of Rights is to the protection of our fundamental personal freedoms.”).

⁸⁴ MAGNUSON, *supra* note 73, at 197-98 (describing the liberalism of John Stuart Mill).

D. From Coase, Through Anarchy, and Back to the Firm

Antitrust is founded on the dichotomy between cooperation inside a “firm” and competition in a “market.”⁸⁵ The boundaries of the firm are thus crucial to determining if the law applies, assessing practices, and assigning liability.⁸⁶ Schrepel poses that, currently, blockchains “ultimately escape . . . antitrust oversight because [they do not] involve any clear power of command and control.”⁸⁷ They are neither firms nor markets, competing with both.⁸⁸ Nor are blockchains incorporated; they possess no legal personhood, while the text of the Sherman Act refers to entities.⁸⁹ The lack of correspondence to a single undertaking is thus doubly problematic.⁹⁰

Let us first dismiss the point regarding legal incorporation. The recent action brought by the Commodity Futures Trading Commission (CFTC) against one of the decentralized autonomous organizations (DAOs) located on the blockchain shows that the law does not allow for an *alegal* vacuum and is prepared to attribute the status of a general partnership or unincorporated association to non-entities.⁹¹ What

⁸⁵ Frank H. Easterbrook, *Limits of Antitrust*, 63 TEX. L. REV. 1, 1 (1984) (“Anti-trust law permits, even encourages, cooperation within a “firm,” for such cooperation is the basis of economic productivity.”). See, e.g., *Copperweld Corp. v. Independence Tube Corp.*, 467 U.S. 752 (1984).

⁸⁶ SCHREPEL, *supra* note 33, at 92.

⁸⁷ *Id.* at 95.

⁸⁸ *Id.* (“Blockchain layer 1 is a transactional institution competing with firms and markets.”).

⁸⁹ 15 U.S.C. §§ 1-2 refer to “persons.” Further, § 7 specifies that:

The word “person,” or “persons,” wherever used in this Act [15 USCS §§ 1 et seq.] shall be deemed to include corporations and associations existing under or authorized by the laws of either the United States, the laws of any of the Territories, the laws of any State, or the laws of any foreign country.

This makes application of the Sherman Act problematic. See Schrepel, *supra* note 9, at 302.

⁹⁰ Mariateresa Maggolino & Laura Zoboli, *Blockchain Governance: The Missing Piece in the Competition Puzzle*, 43 COMPUT. LAW SECUR. REV. 105609, 1, 4 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3954827#.

⁹¹ See *Commodity Futures Trading Comm’n v. Ooki DAO*, No. 3:22-CV-05416, 2022 LEXIS 228820, at *14-23 (N.D. Cal. Dec. 20, 2022); see also *Sarcuni v. bZx DA*, No. 22-CV-618, 2023 U.S. Dist. LEXIS 52245, at *19-28 (S.D. Cal., Mar. 27, 2023). See also Matt Błaszczyk, *Decentralized Autonomous Organizations and Regulatory Competition: A Race Without a Cause*, 99 N.D. L. REV. 107 (2024). On

about the firm? The European Union (“EU”) jurisprudence is instructive that the concept of an *undertaking* is functional, relative, and focused on the activity rather than the legal form.⁹² Indeed, competition law seems to reach economic undertakings “regardless of the legal status of the entity.”⁹³ In the EU, an undertaking is defined as follows:

Any entity carrying on activities of an economic nature, regardless of its legal form, constitutes an undertaking within the meaning of Article 85 of the EEC Treaty. An activity of an economic nature means any activity, whether or not profit-making, that involves economic trade.⁹⁴

Now, it seems that permissionless blockchains are not firms: they facilitate transactions between the users without a central authority.⁹⁵ They do not *engage* in them themselves. In this way, they do not correspond to Coasean theory, since there is no top-down hierarchical command,⁹⁶ and seemingly no structure whose borders delineate what conduct is internal or external.⁹⁷ Thus, they supposedly fall “beyond the oversight of antitrust enforcers,” making the law “mostly

alegality in the context of blockchain technology, see generally Primavera De Filippi et al., *The Alegality of Blockchain Technology*, 41 POL’Y & SOC’Y 358, 358 (2022) (defining alegality as “situated beyond the boundaries of existing legal orders, and therefore, challenging them.”).

⁹² ARIEL EZRACHI, *EU COMPETITION LAW: AN ANALYTICAL GUIDE TO THE LEADING CASES 1* (2018).

⁹³ Case C-41/90, *Höfner & Elser v. Macrotron GmbH*, 1991 E.C.R. I-01979, ¶ 21. See also Case C-364/92, *SAT Fluggesellschaft mbH v. Eurocontrol*, 1994 E.C.R. I-43, ¶¶ 18, 19.

⁹⁴ Commission Decision, *Relating to a Proceeding under Article 85 of EEC Treaty 1992 O.J.(L 326) 43* (EC).

⁹⁵ SCHREPEL, *supra* note 33, at 95.

⁹⁶ See Ronald H. Coase, *The Nature of the Firm*, 4 *ECONOMICA* 386, 387 (2007).

⁹⁷ Analogizing to familiar legal concepts, internal conduct is akin to the use of a firm’s property rights, while external conduct involves a contract excluding competitors. Alan J. Meese, *Monopolization, Exclusion, and the Theory of the Firm*, 89 *MINN. L. REV.* 743, 746 (2005). Broadly speaking, conduct occurring within the firm, such as “decisions on product design, marketing strategies, refusals to buy or sell, and pricing and output,” is seen as competition on the merits and presumed lawful, even if it drives competitors away from the marketplace. *Id.* at 745. External conduct, on the other hand, is presumed unlawful if it significantly impairs or tends to so impair the opportunities of rivals. *Id.* Thus, if there is no firm, it is harder to determine what is lawful, and what is not.

inapplicable to blockchain ecosystems.”⁹⁸ (Private, permissioned blockchains, of course, do not posit a similar problem, and can be categorized as firms more straightforwardly).⁹⁹ Schrepel says that permissionless blockchains’ provision of infrastructure makes them “more than mere market[s]”; they provide more information and eliminate transaction costs.¹⁰⁰ If they are neither markets nor firms, do they constitute an *alegal* entity that competition law cannot reach, like crypto-anarchists proclaim? Is this so, even though there are dangers to competition policy, to destabilization of central banking, financial markets, the administration of commercial agreements, and potential for unlawful activity?¹⁰¹

Transitioning to an answer, we may point out that traditional firms may not necessarily be the “islands of conscious power,” either.¹⁰² To cite another classic work, Alchian and Demsetz write that such characterization is a “delusion.”¹⁰³ Rather, a firm “has no power of fiat, no authority, no disciplinary action any different in the slightest degree from ordinary market contracting between any two people.”¹⁰⁴ That said, blockchains, and organizations based on them, bear a greater resemblance to cooperatives than traditional firms,¹⁰⁵ since there exists a democratic cooperation within the undertaking and,¹⁰⁶ as explored

⁹⁸ SCHREPEL, *supra* note 33, at 102-04.

⁹⁹ *Id.* at 104-07 (Although Schrepel notes that they “must be studied on a case-by-case basis” since the extent of control exercised on private blockchains ranges from “an almost firm-like model to one that is more similar to public permissionless blockchains.”).

¹⁰⁰ *Id.* at 98-99.

¹⁰¹ DE FILIPPI & WRIGHT, *supra* note 7, at 6.

¹⁰² *Cf.* Coase, *supra* note 96, at 388.

¹⁰³ Armen A. Alchian & Harold Demsetz, *Production, Information Costs, and Economic Organization*, 62 AMERICAN ECONOMIC REVIEW 777, 777 (1972).

¹⁰⁴ *Id.* See also Michael Jensen & William Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. OF FINANCIAL ECONOMICS 305, 310 (1976).

¹⁰⁵ Sandeep Vaheesan & Nathan Schneider, *Cooperative Enterprise as an Antimonopoly Strategy*, 124 PENN STATE L. REV. 1, 16 (2019). See also Morshed Mannan, *Fostering Worker Cooperatives with Blockchain Technology: Lessons from the Colony Project*, 11 ERASMUS L. REV. 190 (2018).

¹⁰⁶ Vaheesan and Schneider argue that “competition among large firms should be paired with support for democratic cooperation within firms.” Vaheesan & Schneider, *supra* note 105, at 4. They also define a cooperative as “a business or other collective owned and governed by the people or organizations that benefit from its product, service, or employment, rather than by outside investors seeking solely financial return.” *Id.* at 16.

further below, a similar threat that enforcement against seemingly collusive practices may impair the development of these organizational structures.¹⁰⁷

The claim that permissionless blockchains are immune from antitrust in particular and liability in general, as we have seen, comes from the fact they are decentralized, i.e., that “there is no central entity that either creates or maintains” the blockchain, which is rather governed “on a peer-to-peer basis through the running of open-source software by a network of computers,” while the “code is publicly available, and anyone in the world may propose a change through a standardized proposal process.”¹⁰⁸ Scholars sympathetic to the utopian vision have thus argued that there is “no *place* for default law on the blockchain, unless the blockchain affirmatively lets it in,” and that there is “no *legal intervention point*.”¹⁰⁹ This is a technical obstacle which necessitates a rethinking of how antitrust laws are designed and enforced, as explored in Part IV.

Indeed, some authors argue that although “blockchain technology seems to reduce costs of the type that can otherwise lead to centralization and entrenched market power in digital platforms,” with decentralization reducing the need for antitrust enforcement, it also brings “an unparalleled set of novel challenges,” namely the practical impossibility of any enforcement.¹¹⁰ Decentralization may mean that identifying an entity to hold responsible for market abuses is impossible, while “collusion and price setting between competitors may be harder to detect.”¹¹¹

However, on closer inspection, decentralization of decision-making power is not all that it is made out to be. As a reminder, blockchains are composed of founders and core developers, i.e., the original designers of the software who, at least nominally, do not exercise active control over the blockchain, and while they are the ones implementing the changes into the code, they do not perform a centralized

¹⁰⁷ *Id.* at 26-27.

¹⁰⁸ Angela Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains*, in REGULATING BLOCKCHAIN: TECHNO-SOCIAL AND LEGAL CHALLENGES 58, 60-61 (Philipp Hacker et al. eds., 2019).

¹⁰⁹ Rodrigues, *supra* note 82, at 682.

¹¹⁰ Christian Catalini & Catherine Tucker, *Antitrust and Costless Verification: An Optimistic and a Pessimistic View of Blockchain Technology*, 82 ANTITRUST L.J. 861, 862 (2019).

¹¹¹ *Id.* at 863.

role.¹¹² Then we have miners, who invest computational power and make the blockchain work.¹¹³ In reality, they are aggregated into pools, which “wield considerable power,” having the potential “to make or break a new blockchain by choosing to mine for it.”¹¹⁴ Indeed, some worry that rules will be coded by a few developers with enormous power,¹¹⁵ since in fact there seem to exist “clusters of power or agency within the systems.”¹¹⁶ According to Nouriel Roubini, “decentralization is a myth,” since there exist “massive centralization and concentration of oligopolistic power and cartels among miners, exchanges, developers, wealth holders.”¹¹⁷ Scholars further write that “power is concentrated to critical sites and individuals who sometimes manage the system through ad-hoc negotiations, and who[m] users must therefore implicitly trust.”¹¹⁸ At the same time, to argue that liability simply cannot be assigned (as distinguished from enforced¹¹⁹) seems contrary to the basic rule of law principles and, perhaps more importantly, unrealistic in the face of active enforcement by agencies and private suits.¹²⁰ The law does not tolerate vacuums and, unless we contest the legitimacy of antitrust at large, some enforcement

¹¹² For a recent treatment, see Cesare Fracassi, Moazzam Khoja, & Fabian Schär, *Decentralized Crypto Governance? Transparency and Concentration in Ethereum Decision-Making* (2024), <https://ssrn.com/abstract=4691000>. Cf., e.g., Yesha Yadav, *The Centralization Paradox in Cryptocurrency Markets*, 100 WASH. U. L. REV. 1725 (2023).

¹¹³ Pat Treacy & Alex Latham, *Blockchain and Competition Law*, 41 E.C.L.R 602, 604 (2020).

¹¹⁴ *Id.*

¹¹⁵ Kelvin F. K. Low & Eliza Mik, *Pause the Blockchain Legal Revolution*, 69 ICLQ 135, 139 (2020).

¹¹⁶ Angela Walch, *Deconstructing ‘Decentralization’: Exploring the Core Claim of Crypto Systems*, in CRYPTO ASSETS: LEGAL AND MONETARY PERSPECTIVES 39, 43 (Chris Brummer ed., 2019).

¹¹⁷ Nouriel Roubini, *Crypto is the Mother of All Scams and (Now Busted) Bubbles While Blockchain is the Most Over-Hyped Technology Ever, No Better than a Spreadsheet/Database*, N.Y.U. (October 2018), <https://www.banking.senate.gov/imo/media/doc/Roubini%20Testimony%202010-11-18.pdf>.

¹¹⁸ Gili Vidan & Vili Lehdonvirta, *Mine the Gap: Bitcoin and the Maintenance of Trustlessness*, 21 NEW MEDIA & SOC’Y 42, 42 (2019).

¹¹⁹ See *infra* Part III.

¹²⁰ See Dirk A. Zetzsche et al., *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018 U. ILL. L. REV. 1361, 1396 (2018).

mechanism will still be necessary,¹²¹ though it may demand a doctrinal change, to update the law's concept of a firm or undertaking, locating the relevant antitrust wrongdoers.

E. The Blockchain “Nucleus”

Schrepel proposes that competition law can solve this problem through invention of a novel legal fiction.¹²² Each group participating in the governance of a permissionless blockchain—core developers, users, and miners—can “achieve a form of control over the blockchain by collaborating, by circumventing (some of) the constraints imposed on them, and by changing them in the long run.”¹²³ Antitrust can identify those concentrations of power and impose liability if the *nucleus*, as Schrepel calls it, engages in anticompetitive conduct, discussed in detail in Part III.¹²⁴ The assessment of who engages in such practices can only be made on a case-by-case basis, using the horizontal power as a metric, to see when a particular group attempts to incentivize others to behave in a certain way.¹²⁵ Whether this is, in fact, a novel legal fiction, or simply following the functional approach to the definition of an undertaking, though in a more challenging economic environment, is up for debate.

Moreover, reverting from the doctrine back to antitrust theory, Schrepel argues that “antitrust law and blockchain ecosystems seek decentralization at two different levels.”¹²⁶ Clearly, antitrust, as state law, prohibits certain categories of conduct to advance a competitive economy, while blockchain as a non-state, technological architecture, provides the code, voting mechanisms, etc., to advance similar goals, but only where “code allows.”¹²⁷ The intersection of these different regulatory modalities—long studied in transnational and legal pluralist

¹²¹ Giovanna Massarotto, *Antitrust in the Blockchain Era*, 1 NOTRE DAME J. ON EMERGING TECH. 252, 254 (2020) [hereinafter Massarotto, *Antitrust in the Blockchain Era*].

¹²² SCHREPEL, *supra* note 33, at 102 (“It is thus necessary to create a new legal fiction around blockchain layer 1 so that the law can be (re)applied.”).

¹²³ *Id.* at 123 (footnotes omitted).

¹²⁴ *Id.* at 124.

¹²⁵ *Id.* at 127; *see also* Maggiolino & Zoboli, *supra* note 90, at nn.5, 6 (writing that the assigning of liability necessitates fact specific inquiry into who controls the blockchain and what governance model is implemented).

¹²⁶ SCHREPEL, *supra* note 33, at 75.

¹²⁷ *Id.*

approaches to private governance¹²⁸—may seem novel. In fact, it is the bread and butter of antitrust law to tackle private agreements if they have anticompetitive effect but not if they further the competitive process.¹²⁹ For example, scholars noted that attempts at private ordering that may advance social welfare, such as in the context of resource conservation—but conflict with antitrust doctrine—prevent the emergence of community-based rules and private regimes (e.g., in fisheries, where agreements to limit harvests amount to cartels).¹³⁰ Finally, whether the agreement is in natural language or code is immaterial. The skeptically inclined may then repeat, after Low and Mik, that the “promised blockchain legal revolution appears to be a damp, and regrettably widely distributed, squib.”¹³¹

III. BLOCKCHAIN: THE GOOD, THE BAD, AND THE ANTITRUST DOCTRINE

We have established that blockchains are not beyond the reach of competition law. We have also noted that permissionless blockchains carry a pro-competitive potential. They seem to bring about greater structural decentralization, breaking with the paradigm of big Internet platforms, which are of concern to at least some antitrust scholars and policymakers.¹³² At the same time, others note that blockchains further enable already recognized anticompetitive practices and give rise to new ones related to the technology (as discussed further below).¹³³ The technology presents doctrinal challenges, making it difficult to define the relevant market, characterize dominance, and then

¹²⁸ See generally PEER ZUMBANSEN, *THE OXFORD HANDBOOK OF TRANSNATIONAL LAW* (2021); MICHAEL W. DOWDLE, *TRANSNATIONAL LAW: A FRAMEWORK FOR ANALYSIS* (2022).

¹²⁹ *Morrison v. Murray Biscuit Co.*, 797 F.2d 1430, 1437 (7th Cir. 1986) (“The purpose of antitrust law, at least as articulated in the modern cases, is to protect the competitive process as a means of promoting economic efficiency.”).

¹³⁰ See Jonathan H. Adler, *Legal Obstacles to Private Ordering in Marine Fisheries*, 8 ROGER WILLIAMS U. L. REV. 9, 29 (2002); see also Jonathan H. Adler, *Conservation Through Collusion: Antitrust as an Obstacle to Marine Resource Conservation*, 61 WASH. & LEE L. REV. 3, 24 (2004).

¹³¹ Low & Mik, *supra* note 115, at 32.

¹³² See Ioannis Lianos, *Blockchain Competition*, UCL CENTRE FOR LAW, ECONOMICS AND SOCIETY (Research Paper 08/2018), <https://ssrn.com/abstract=3257307>, at 42 (calling it an “architectural advantage”).

¹³³ Schrepel, *supra* note 9, at 306.

to attribute liability for anticompetitive practices.¹³⁴ The methodological starting point can be the *nucleus* proposal examined above, which delineates the undertaking and can take into account the number of users, transactions recorded, the number of blocks, and the revenues, to engage in fact-specific findings of abuse.¹³⁵ But what anticompetitive conduct are we to expect?

A. Collusion

Section One of the Sherman Act prohibits conspiracies that unreasonably restrain interstate or foreign trade.¹³⁶ This Section intends to prevent artificial centralization of the market, one which does not stem from the competitive process, through collusive, illegal agreements.¹³⁷ The most extreme forms of cartel behaviors are illegal *per se*,¹³⁸ while others are subject to the rule of reason, which requires a showing that the “practice imposes an unreasonable restraint on competition, taking into account a variety of factors,”¹³⁹ whether in horizontal, hub-and-spoke, or vertical contexts.¹⁴⁰ Similar objectives are achieved by Article 101 of the Treaty on the Functioning of the European Union (“TFEU”).

1. Are Public Blockchains Collusive?

Creation of a permissionless blockchain is, arguably, either an agreement (which, in competition law is defined broadly) or a decision by an association of undertakings.¹⁴¹ Thus, it is interesting whether the

¹³⁴ *Id.* at 301.

¹³⁵ *Id.* at 305.

¹³⁶ 15 U.S.C. § 1; *see also* Quality Auto Painting Ctr. of Roselle, Inc. v. State Farm Indem. Co., 917 F.3d 1249, 1260 (11th Cir. 2019).

¹³⁷ SCHREPEL, *supra* note 33, at 69.

¹³⁸ United States v. Socony-Vacuum Oil Co., 310 U.S. 150, 223 (1940) (“[A] combination formed for the purpose and with the effect of raising, depressing, fixing, pegging, or stabilizing the price of a commodity in interstate or foreign commerce is illegal *per se*.”).

¹³⁹ Spanish Broad. Sys. of Fla., Inc. v. Clear Channel Commc’ns, Inc., 376 F.3d 1065, 1071 (11th Cir. 2004).

¹⁴⁰ United States v. Apple, Inc., 791 F.3d 290, 322 (2d Cir. 2015).

¹⁴¹ SCHREPEL, *supra* note 33, at 142; *see* Case T-41/96, Bayer AG. v. Comm’n, 2000 E.C.R. II-3444; JOHN H. SHENEFIELD & IRWIN M. STELZER, THE ANTITRUST LAWS: A PRIMER 45 (4th ed. 2001) (In the U.S., an “agreement can be a written document or merely an oral exchange of assurances, or even hints, that competitors will

characteristics of blockchains make them anticompetitive. Relevantly, blockchains make pseudonymized data about transactions available to everyone—a record of all transactions is available to everyone, so that the ledger is complete, certain, and identical, which is the basis of the “consensus mechanism.”¹⁴² While the scope of the information about transactions is limited and rendered obscure through the use of cryptographic pseudonymization, it can nonetheless be traced back to the users with appropriate decrypting methods.¹⁴³ In this way, blockchains turn “private information into genuinely public information,” making “markets more transparent, with all the pros and cons that entail.”¹⁴⁴ Such an extensive flow of information could be suspect from antitrust law’s perspective.¹⁴⁵

Indeed, according to Weinstein, “[e]ven without explicit collusive agreements, blockchain’s enhanced information-sharing capabilities might facilitate tacit collusion among participants.”¹⁴⁶ Massarotto further notes that permissioned blockchains “create the perfect conditions for competitors to engage in cartels,” while smart contracts have the potential to “automatize the punishment for any cartel’s deviation.”¹⁴⁷

This seems to be an exaggeration that misidentifies the nature of the information shared, which is public, that is available to all participants in the blockchain, and regards actual prices, rather than future prices or activities, the sharing of which is not prohibited.¹⁴⁸ Indeed, in the United States, the exchange of public information, of itself, is

pursue some coordinated plan. Furthermore, an agreement can be proven by using only circumstantial evidence.”).

¹⁴² COMMODITY FUTURES TRADING COMMISSION, *DECENTRALIZED FINANCE* 23 (2024).

¹⁴³ See Michèle Finck, *Blockchains and Data Protection in the European Union*, 1 EUR. DATA PROT. L. REV. 13 (2018).

¹⁴⁴ SCHREPEL, *supra* note 33, at 143.

¹⁴⁵ Herbert Hovenkamp, *Antitrust and Information Technologies*, 68 FLA. L. REV. 419, 420-21 (2016) (“particular uses of information threaten competition when they enable firms to coordinate price, output, or innovation. . . . [T]echnological change can both facilitate and undermine the use of information for anticompetitive practices.”).

¹⁴⁶ Weinstein, *supra* note 32, at 538.

¹⁴⁷ Giovanna Massarotto, *Can Antitrust Trust Blockchain?*, in ALGORITHMIC ANTITRUST 121, 122 (Aurelien Portuese ed., 2022) (hereinafter Massarotto, *Can Antitrust Trust Blockchain?*).

¹⁴⁸ Thibault Schrepel, *Collusion by Blockchain and Smart Contracts*, 33 HARV. J.L. & TECH. 117, 132 (2019).

not seen as anticompetitive, and it demands an evaluation of actual evidence of anticompetitive harm under the rule of reason.¹⁴⁹ Similarly, in the EU, the sharing of “genuinely public information [is] unlikely to constitute an infringement of Article 101.”¹⁵⁰ Since the information exchanged is publicly available, “the risk of its exchange between competitors seems low.”¹⁵¹ Reasoning from similar premises, the U.S. Federal Maritime Commission has granted antitrust enforcement exemptions to several blockchain supply chain shipping consortia, allowing them to cooperate in providing data for use on the platforms.¹⁵² Finally, although in the EU even unilateral disclosures of information relevant to the market can amount to a concentrated practice,¹⁵³ a violation would still require a finding of an anticompetitive object or effect. This seems unlikely, since the sharing of the limited scope of information is necessary to participate in a fluid and decentralized market, which is open to everyone.¹⁵⁴ Thus, we conclude, that the mere creation of a public blockchain will not be deemed collusive, whether in the U.S. or the EU.

¹⁴⁹ *United States v. U.S. Gypsum Co.*, 438 U.S. 422, 438 (1978); Schrepel, *supra* note 148, at 132.

¹⁵⁰ Guidelines on the Applicability of Article 101 of the Treaty on the Functioning of the European Union to Horizontal Co-operation Agreements, 92, O.J. (2011) C 11/1 (Jan. 14, 2011). *Cf.* Guidelines on the Applicability of Article 101 of the Treaty on the Functioning of the European Union to Horizontal Co-Operation Agreements, O.J. 400, 425 (2023) C 259/01 (July 21, 2023).

¹⁵¹ SCHREPEL, *supra* note 33, at 140 (quoting OECD, Information Exchanges Between Competitors under Competition Law, DAF/COMP(2010)37, 296 (2010)).

¹⁵² *See* The Global Shipping Business Network Agreement, FMC Agreement No. 201344, FEDERAL MARITIME COMMISSION <https://www2.fmc.gov/FMC.Agreements.Web/Public/AgreementHistory/29502>; The TradeLens Agreement, FMC Agreement No. 201328, FEDERAL MARITIME COMMISSION <https://www2.fmc.gov/FMC.Agreements.Web/Public/AgreementHistory/26452>; *see also* Jonathan Mollod & Jeffrey D. Neuburger, *Another Blockchain Supply Chain Shipping Consortium Files for Federal Antitrust Exemption*, PROSKAUER (June 3, 2020), <https://www.proskauer.com/blog/another-blockchain-supply-chain-shipping-consortium-files-for-federal-antitrust-exemption>.

¹⁵³ *Joined Cases T-202/98, T-204/92 and T-207/98, Tate & Lyle plc v. Comm’n*, 2001 E.C.R. II-2040, ¶¶ 35, 54, 61.

¹⁵⁴ SCHREPEL, *supra* note 33, at 144; *see also* Marixenia Davilla, *Unravelling the Complexity of Blockchain and EU Competition Law*, 13 J. OF EUR. COMPETITION L. & PRAC. 387 (2022).

While the creation of a public blockchain is not collusive, it can nonetheless facilitate collusive practices.¹⁵⁵ This can be done straightforwardly: a cartel can use a blockchain to store and exchange information among its members, just like it would use any other information-sharing technology.¹⁵⁶ The only novelty is technological; it is arguably easier to coordinate if the recorded information is stored in the same place, without any member of the cartel being able to hide it from the others.¹⁵⁷ Secondly, a cartel can implement its agreement with the use of smart contracts, effectively ensuring that the members comply with the technologically perfected agreement.¹⁵⁸ Although there is no doctrinal challenge here, the potential for abuse is technologically magnified. Smart contracts ensure stability of the collusive agreement, which is difficult to stop once the smart contract code is launched, and difficult to detect, since the publicly shared information does not reveal whether an agreement is legal or not.¹⁵⁹

Finally, while it is not likely that a public and permissionless blockchain is of itself collusive, unless a plaintiff shows concrete economic harm, this is a largely structural conclusion: it stems from the fact that permissionless blockchains are open for all to entry, that the process is competitive and decentralized, while the power to control the blockchain is distributed among all participants. As we have already noted,¹⁶⁰ however, in practice, miners are grouped into pools—e.g., with less than a dozen of such groups controlling the Bitcoin

¹⁵⁵ Izabella Kaminska, *Exposing the “If We Call it a Blockchain, Perhaps it Won’t be Deemed a Cartel?” Tactic*, FIN. TIMES: ALPHAVILLE (May 11, 2015, 12:59 PM), <https://ftalphaville.ft.com/2015/05/11/2128849/exposing-the-if-we-call-it-a-blockchain-perhaps-it-wont-be-deemed-a-cartel-tactic> (“[What the technology really facilitates is cartel management for groups that don’t trust each other but which still need to work together if they’re to protect the value and stability of the markets they serve.”).

¹⁵⁶ Schrepel, *supra* note 148, at 141.

¹⁵⁷ *Id.*

¹⁵⁸ Schrepel, *supra* note 148, at 142; David C. Kully & Josias N. Dewey, *Blockchain Collaborators Should Be Attuned to Potential Antitrust Issues*, THOMSON REUTERS (Mar. 2017), <https://legalsolutions.thomsonreuters.com/law-products/news-views/corporate-counsel/blockchain-collaborators-attuned-to-potential-antitrust> (arguing that the technology could be used to “establish industry wide prices and ensure that members adhere to any agreement.”).

¹⁵⁹ Schrepel, *supra* note 148, at 143 (“Blockchain provides help on both fronts by preventing the colluders from cheating on the agreement and by reducing the detection risk.”).

¹⁶⁰ *See supra* Part II.

chain.¹⁶¹ The more concentrated the power structures on permissionless blockchains become, the greater the risk of collusive behavior, including bribery of other voters (or rather, their pools) and coordination of economic activity.¹⁶² This becomes a problem when there emerges a majority of miners that can effectively control the blockchain—and, importantly, change its rules and the record of transactions in what is called a 51% attack.¹⁶³ In this scenario, we see miners deciding to update the code of the blockchain by changing which transactions are seen as valid. If this is accepted by all participants, then the software is overwritten without contention; if not, the blockchain splits, with the majority creating a new one and abandoning the previous one (this is also known as a *hard fork*).¹⁶⁴

While these forks are difficult to conduct on the biggest blockchains (but can more easily be conducted on smaller ones, especially private chains, where the 51% majority can be convinced more easily), they have already happened on both Bitcoin and Ethereum, with each fork raising doubts on whether blockchains are indeed immutable and trustless.¹⁶⁵ This not only reveals an emergence of “bigness” in the seemingly decentralized structures but also puts into doubt whether the users can trust the code without the law controlling the effects of illicit changes.¹⁶⁶ Should all hard forks be treated as collusive? After all, those who do not follow the majority are excluded from the newly created blockchain, while their assets lose value. One cryptocurrency exchange announced that it had lost Ether worth over \$14 million as a result of the Ethereum fork.¹⁶⁷ This is unlikely: antitrust orthodoxically protects competition, not competitors.¹⁶⁸ At the same time, it is not difficult to envisage a scenario in which the pooled miners and

¹⁶¹ DE FILIPPI & WRIGHT, *supra* note 7, at 180.

¹⁶² SCHREPEL, *supra* note 33, at 150.

¹⁶³ Schrepel, *supra* note 148, at 135; Lianos, *supra* note 132, at 69.

¹⁶⁴ Werbach, *supra* note 29, at 103.

¹⁶⁵ See, e.g., Sangita Gazi, *In Code We Trust: Blockchain's Decentralization Paradox*, VAND. J. ENT. & TECH. L. (forthcoming 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4769723, at 25.

¹⁶⁶ Piotr Tereszkievicz, *Digital Platforms*, in CAMBRIDGE HANDBOOK, DE FILIPPI & WRIGHT, *supra* note 7, at 143, 170.

¹⁶⁷ Werbach, *supra* note 46, at 516.

¹⁶⁸ See, e.g., Louis B. Schwartz, *Justice and Other Non-Economic Goals of Antitrust*, 127 U. PA. L. REV. 1076, 1078 (1979) (This phrase has been an object of stark criticism from the broadly construed political antitrust movement.).

developers conspire together to the detriment of others.¹⁶⁹ Indeed, authors have argued that the “migration of miners across platforms may be subject to significant scrutiny by competition authorities, particularly if certain blockchains are allowed to fail or are deliberately bypassed by an exploitative mining pool.”¹⁷⁰ We will analyze how these novel issues played out in the case of *United American Corporation v. Bitmain, Inc.*¹⁷¹ and discuss how self-regulatory measures, which blockchains can incorporate to prevent anticompetitive abuses, challenge antitrust doctrine further.

2. *Bitmain*

So far, we have had few competition cases dealing with blockchain. In *Bitmain*, the plaintiffs alleged that certain miners violated the Sherman Act by conspiring to take control of the blockchain, in relation to an ongoing fork.¹⁷² Put simply, there was an ongoing vote regarding the future of the blockchain, and those who lost and decided not to follow the majority, created a new one, with a lesser or at least uncertain economic value, as it often goes. Here, plaintiffs alleged that “a number of investors, mining pools . . . crypto-exchanges, and protocol developers colluded to get as many miners as possible to support the Bitcoin ABC fork over the Bitcoin SV fork.”¹⁷³ The case, while akin to familiar litigation involving market manipulation,¹⁷⁴ is not very instructive, since the claim was dismissed without being specific as to what paradigm of collusive activity occurred,¹⁷⁵ failed to specify facts amounting to a conspiracy,¹⁷⁶ and did not expressly allege an agreement.¹⁷⁷ At the same time, the dismissal of the claim by the court could be seen, at the very least, as supporting our conclusion that blockchains are not in and of themselves collusive.

Interestingly, the court engaged in the discussion of what the relevant product market would be: is it a particular cryptocurrency,

¹⁶⁹ See, e.g., Schrepel, *supra* note 148, at 149.

¹⁷⁰ Treacy & Latham, *supra* note 113, at 604.

¹⁷¹ 530 F. Supp. 3d 1241 (S.D. Fla. 2021).

¹⁷² *Id.*

¹⁷³ Stylianou, *supra* note 12.

¹⁷⁴ Treacy & Latham, *supra* note 113, at 606.

¹⁷⁵ *United Am. Corp. v. Bitmain, Inc.*, 530 F. Supp. 3d 1241, 1256 (S.D. Fla. 2021).

¹⁷⁶ *Id.*

¹⁷⁷ *Id.* at 1257.

Bitcoin Cash, or was it within the larger market of some or all cryptocurrencies?¹⁷⁸ The court opined that:

The fact that “each form of cryptocurrency has distinctive characteristics” says little. This is true for many products that compete in a market. UAC’s allegation that Bitcoin Cash is “unique” because of its utility for peer-to-peer daily transactions and that it is the most widely adopted form of a cash-like cryptocurrency leaves us hanging. It tells us nothing that would allow us to discern the extent to which consumers prefer Bitcoin Cash over the multitude of other cryptocurrencies.¹⁷⁹

Furthermore, the court found that the plaintiffs did not characterize the harm they suffered sufficiently.¹⁸⁰ Naturally, this is an early, district court case, though others, such as *In re Tether and Bitfinex Crypto Asset Litigation* are following.¹⁸¹ What we can take away is an indication that the courts will be wary of constructing the relevant market too narrowly as to not stifle innovation and competition. On the other hand, we may question whether reliance on “static conceptions of competition focused entirely on minimizing deadweight loss—the loss of total welfare or social surplus due to monopoly pricing,” remains the appropriate approach.¹⁸²

Moreover, the high evidentiary burden imposed on private actions in such complex environments, for better or worse,¹⁸³ shows that competition law may not become the primary domain of power struggle over permissionless blockchains.¹⁸⁴ The high bar to establish a

¹⁷⁸ *Id.* at 1267-68.

¹⁷⁹ *Id.* at 1269.

¹⁸⁰ *Id.* at 1271.

¹⁸¹ *In re Tether & Bitfinex Crypto Asset Litig.*, 576 F. Supp. 3d 55 (S.D.N.Y. 2021); *see infra* note 225.

¹⁸² Victor Martinez, Note, *The Sherman-Twombly Hard Fork: The Plausibility of Regulating Competition in Decentralized Finance Markets*, 60 HOUS. L. REV. 495, 517 (2022) (“contrary to the original intent of the Supreme Court, antitrust plaintiffs face significant barriers to court access posed by current federal pleading standards.”).

¹⁸³ *Id.* at 510.

¹⁸⁴ Stylianou, *supra* note 12 (“To uphold...that mining mobilization can underpin an antitrust offense would risk serving as an implicit acknowledgement of the legal bindingness of cryptocurrency whitepapers and their decentralization and democratic ideals.”).

monopolistic violation in the U.S. is not just evidentiary,¹⁸⁵ but as *Epic Games v. Apple*¹⁸⁶ shows, in two-sided markets, if the total number of transactions is increasing, then a finding of market power is precluded.¹⁸⁷ In other words, the output is not restricted,¹⁸⁸ and forking, in and of itself, is unlikely to be found abusive.

Furthermore, while the case draws parallels with litigation concerning uneconomic bids from energy traders or false quotes from LIBOR traders, it raises the question of what constitutes a harm in such markets: “Can collusion to influence . . . a cryptocurrency’s governance system result in harm of the kind that antitrust law would acknowledge?”¹⁸⁹ Were the plaintiffs hurt as an investor with decreased sales in offerings or as a miner with lowered profits?¹⁹⁰ One commentator claimed that the case shows that “conventional theories of antitrust harm and judicial review are patently inadequate to capture and define potentially anticompetitive conduct occurring” in blockchain markets.¹⁹¹ Others dismissed this as a misunderstanding: antitrust protects competition, not competitors.¹⁹²

3. *Are Private Blockchains Collusive?*

Having examined permissionless blockchains, we turn to private, permissioned chains. Clearly enough, they pose a greater risk to competition: they are gatekept by differing conditions of access, with the founders having a greater degree of centralized power, and thus the potential to engage in collusive behaviors.¹⁹³ If the conditions of access have an anticompetitive effect, their creation may be considered a

¹⁸⁵ See Fed. Trade Comm’n v. Meta Platforms Inc., No. 5:22-CV-04325, 2023 WL 2346238, at *30 (N.D. Cal. Feb. 3, 2023).

¹⁸⁶ No. 21-16506, 2023 WL 3050076 (9th Cir. Apr. 24, 2023).

¹⁸⁷ Marshall Steinbaum, *Establishing Market and Monopoly Power in Tech Platform Antitrust Cases*, THE ANTITRUST BULLETIN, at 2.

¹⁸⁸ See *Ohio v. Am. Express Co.*, 138 S. Ct. 2274, 2278 (2018).

¹⁸⁹ Stylianou, *supra* note 12.

¹⁹⁰ Treacy & Latham, *supra* note 113, at 606.

¹⁹¹ Martinez, *supra* note 182, at 511.

¹⁹² Maggolino & Zoboli, *supra* note 90, at 10 (“These claims, however, are not relevant in an antitrust perspective. Antitrust law does not protect competitors, but competition, and the exclusion of a group of firms from a blockchain is not equal to excluding those same firms from the market where blockchains are offered.”).

¹⁹³ See SCHREPEL, *supra* note 33, at 133. See also *infra* sub-section E.

concerted refusal to deal, or as market sharing.¹⁹⁴ Indeed, an exclusion from the blockchain can also be considered an abuse of collective dominance, akin to the case of *Laurent Piau v. Commission of the European Communities*, in which there was an exclusion of agents by FIFA.¹⁹⁵

Moreover, even if the conditions of access are not anticompetitive, the potential for collusion is greater than on permissionless chains. We noted that permissionless blockchains were difficult to modify—forking requires a majority of participants to agree in a democratic vote for the change in rules, pooling and emergent centralization notwithstanding—but such changes are easier to conduct on permissioned chains. Here, the core developers (i.e., the gatekeepers) can use different methods to identify the voters and attempt to sway their decision,¹⁹⁶ exclude some participants from the blockchain, or impose a single client after consultation with select participants.¹⁹⁷ We could see, for example, a private ledger composed of four firms that decided to exclude one of them from the ledger, a worry which arose in the seemingly failed Facebook Libra project.

B. Permissioned Blockchains: The Case of Libra

As we have seen, permissioned blockchains demand a closer antitrust scrutiny, given their structural characteristics and a greater potential for abuse.¹⁹⁸ These ledgers can be owned by corporations, in fact extending rather than undermining the challenges of the platform economy.¹⁹⁹ Unsurprisingly, significant worries ensued when Facebook announced its blockchain-based payment system, Libra, a permissioned system (admittedly, with a vague promise that with time,

¹⁹⁴ SCHREPEL, *supra* note 33, at 145.

¹⁹⁵ See Case T-193/02, *Laurent Piau v. Comm'n*, 2005 E.C.R. II-209.

¹⁹⁶ SCHREPEL, *supra*, note 33, at 153. Schrepele adds that we should “pay close attention to forks resulting from an external group trying to weaken a blockchain.” *Id.* at 157.

¹⁹⁷ *Id.* at 154.

¹⁹⁸ Thibault Schrepele, *Libra: A Concentrate of “Blockchain Antitrust,”* 118 MICH. L. REV. 160, 163 (2020).

¹⁹⁹ See Michele Benedetto Neitz, *The Influencers: Facebook’s Libra, Public Blockchains, and the Ethical Considerations of Centralization*, 21 N.C. J.L. & TECH. 41 (2019); Pedro Aranguez-Diaz, *A New Opportunity for Digital Competition: Facebook, Libra, and Antitrust*, 50 STETSON L. REV. 199 (2020).

the ledger was to become permissionless).²⁰⁰ Called variously a “monopoly of the wealthy” or the “centralized wolf in decentralized sheep’s clothing,”²⁰¹ expected by some to be “the greatest anti-competitive trust case in history,”²⁰² the project sparked a formal investigation of the European Commission regarding its potential anticompetitive behavior.²⁰³ Commentators worried that Meta would be able to select members and change the protocol, raising concern over possibility of subjective grounds of membership denial,²⁰⁴ and over creation of “competition restrictions” on the information exchanged, and on the use of consumer data.²⁰⁵ This structural worry mirrors the broader concern that antitrust policymakers and scholars have expressed over dominant Internet platforms.²⁰⁶ At the same time, there is a doctrinal blessing in disguise: if a single entity manages a permissioned blockchain, there is power to apply Article 102 or Section 2 in a straightforward way, should it engage in anticompetitive conduct.²⁰⁷ Such blockchains are said to either mimic firms, industry consortia, or joint ventures, with exclusionary conduct, e.g., falling squarely into the category of a boycott.²⁰⁸

C. Monopolization

Section 2 of the Sherman Act prohibits “monopolization” of the relevant market (together with an attempt or conspiracy to monopolize),²⁰⁹ while Article 102 of the Treaty on the Functioning of the

²⁰⁰ *Id.* at 165-66.

²⁰¹ Evan Miller, *A Tale of Two Regulators: Antitrust Implications of Progressive Decentralization in Blockchain Platforms*, 77 WASH. & LEE L. REV. 387, 399 (2021).

²⁰² Bronwyn Howell, *Blockchain Node Consolidation: Should We Be Concerned?*, AEI IDEAS (June 28, 2019), <https://www.aei.org/technology-and-innovation/innovation/blockchain-node-consolidation-should-we-be-concerned/>.

²⁰³ Lydia Beyoud & Aoife White, *Facebook’s Libra Currency Gets European Union Antitrust Scrutiny*, BLOOMBERG (Aug. 20, 2019), <https://www.bloomberg.com/news/articles/2019-08-20/facebook-s-libra-currency-gets-european-union-antitrust-scrutiny>.

²⁰⁴ *Id.* See *Northwest Wholesale Stationers, Inc. v. Pacific Stationery & Printing Co.*, 472 U.S. 284, 295-98 (1985).

²⁰⁵ Miller, *supra* note 201, at 400.

²⁰⁶ See generally WU, *supra* note 59.

²⁰⁷ Maggiolino & Zoboli, *supra* note 90, at 9.

²⁰⁸ *Id.* at 10.

²⁰⁹ 15 U.S.C. § 2; SHENEFIELD & STELZER, *supra* note 141, at 36 (“[a]ttempted monopolization is the use of improper tactics to attain monopoly status within a

European Union (TFEU) prohibits “abuse” of market power by dominant firms, who have a special duty.²¹⁰ The latter’s focus is mostly on the *ex ante* power,²¹¹ while in the US, it is equally important to determine the *ex post* increase through conduct which is not competition on the merits,²¹² also known as the purposeful act requirement.²¹³ In both jurisdictions, the first step is to define the relevant product market and the relevant geographic market. In the EU, to make out an Article 102 challenge, what must be established is: (1) a dominant position with respect to the relevant market and relevant product, i.e., a finding of the power to prevent effective competition being maintained on the relevant market, found through several relative and absolute indicia;²¹⁴ and (2) a characterization of the conduct as abusive.²¹⁵ The U.S. requirement of both the monopoly power and exclusionary, anticompetitive conduct,²¹⁶ had meant that it took a narrower approach.²¹⁷ This

market; monopolization is the use of improper tactics to attain or maintain monopoly status or to extend it still further.”).

²¹⁰ See Case T-612/17, *Google & Alphabet v. Comm’n (Google Shopping)* ECLI:EU:T:2021:763 (Nov. 10, 2021); Case T-219/99, *British Airways v. Comm’n of the Eur. Cmty.*, 2003 E.C.R. II-5925 (specifying that while dominant firms can look after their own self-interest, they must also conform to standards of competition, and thus abusive practices tied to their economic power will fall foul of Article 102 TFEU).

²¹¹ Case C-413/14, *Intel Corp. v. Comm’n*, ECLI:EU:C:2017:632, ¶142 (Sept. 6, 2017) (“[B]y [its] very nature capable of restricting competition.”).

²¹² See A. Douglas Melamed, *Antitrust Law Is Not That Complicated*, 130 HARV. L. REV. F. 163, 166 (2017) (Delineating three elements of the US test: “(i) increased market power, (ii) conduct that is not competition on the merits, and (iii) a causal connection between the two.”).

²¹³ *United States v. Grinnell Corp.*, 384 U.S. 563 (1966).

²¹⁴ Case 27/76, ¶65, *United Brands v. Comm’n*, 1978 E.C.R. 0207. See also Case 85/76, *Hoffman La Roche & Co. v. Comm’n*, 1979 E.C.R. 464.

²¹⁵ See *Bundeskartellamt*, Decision B6-22/16 (Facebook); Case C-7/97, *Oscar Bronner v. Mediaprint Zeitungs und Zeitschriftenverlag*, 1998 I-07791.

²¹⁶ *United States v. Grinnell Corp.*, 384 U.S. 563, 570-71 (1966) (“The offense of monopoly under § 2 of the Sherman Act has two elements: (1) the possession of monopoly power in the relevant market and (2) the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident.”).

²¹⁷ *Verizon Commc’ns Inc. v. L. Offs. of Curtis V. Trinko*, 540 U.S. 398, 407 (2004) (“The mere possession of monopoly power, and the concomitant charging of monopoly prices, is not only not unlawful . . . it is an important element of the free-market system. The opportunity to charge monopoly prices—at least for a short period—is what attracts “business acumen” in the first place; it induces risk taking that produces innovation and economic growth.”).

approach is evident, e.g., in the *Google & Alphabet v. Commission (Google Shopping)* saga.²¹⁸ A violation can be proven either through a direct finding of the power to raise prices or exclude competition²¹⁹ or indirectly, based on the substantial share of a relevant market.²²⁰

D. Permissionless Blockchains

This Article began with the hope that permissionless blockchains bring radical decentralization.²²¹ Since in permissionless blockchains there is no one single entity which verifies transactions or acts as an intermediary, the potential for abuse is minimal.²²² Some go as far as to claim “there is no point in discussing the monopoly power if nobody can actually exercise it.”²²³ Instead, what happens is power diffusion, since decentralized decision-making makes abuses virtually impossible, even if the particular blockchain was dominant on the market.²²⁴ Indeed, because of public blockchains’ design, there is “no real possibility of implementing unilateral strategies . . . unless they have been designed in such a way from the day they are created.”²²⁵

²¹⁸ Case T-612/17, *Google & Alphabet v. Comm’n (Google Shopping)* ECLI:EU:T:2021:763 (Nov. 10, 2021); *see generally* ARIEL EZRACHI, *COMPETITION AND ANTITRUST LAW: A VERY SHORT INTRODUCTION*, 99-105 (2021).

²¹⁹ *United States v. E.I. du Pont de Nemours & Co.*, 351 U.S. 377, 391 (1956); *FTC v. Ind. Fed’n of Dentists*, 476 U.S. 447, 460-61 (1986); *Aspen Skiing Co. v. Aspen Highlands Skiing Co.*, 472 U.S. 585, 605 n.32 (1985) (“‘exclusionary’ comprehends, at the most, behavior that not only (1) tends to impair the opportunities of rivals, but also (2) either does not further competition on the merits or does so in an unnecessarily restrictive way.”).

²²⁰ *United States v. Aluminum Co. of Am.*, 148 F.2d 416, 424 (2d Cir. 1945) (“The percentage we have already mentioned- over ninety- . . . is enough to constitute a monopoly; it is doubtful whether sixty or sixty-four percent would be enough; and certainly thirty-three per cent [sic] is not.”).

²²¹ *See, e.g., Sinclair Davidson et al., Blockchains and the Economic Institutions of Capitalism*, 14 J. INSTITUTIONAL ECON. 639, 449 (2018) (“Distributed ledgers are a technology of decentralisation. . . . Blockchains create distributed systems by eliminating centralization that was previously needed for reconciliation or consensus on a ledger with an alternative technology for achieving consensus about economic data.”).

²²² *See Pike & Capobianco, supra* note 45, at 9 (“competition agencies would be well-advised not to spend time worrying about decentralised permissionless blockchains”).

²²³ Maggiolino & Zoboli, *supra* note 90, at 9.

²²⁴ *See id.*

²²⁵ Schrepel, *supra* note 9, at 307.

Moreover, since all transactions are publicly recorded, the number of anticompetitive practices is expected to be lower than in other markets.²²⁶ A public permissionless blockchain cannot easily engage in exclusionary abuses, such as refusal to deal,²²⁷ since no “deliberate or exclusive user selection is necessarily possible.”²²⁸ Similarly, tying or bundling is unlikely to be seen on public blockchains, which can be freely accessed or used.²²⁹

E. Private, Permissioned Blockchains

Anticompetitive practices are, however, possible on private blockchains.²³⁰ Private blockchains, especially those created by for-profit companies could, for example, require the creation of an account on another platform to connect to its blockchain or to get tokens.²³¹ Moreover, “[p]redatory innovation is expected on private blockchains and may become a common practice, since it can be implemented at no cost by simply modifying the blockchain code,” thus “highlight[ing] the need to tackle this practice using an effective regime.”²³² Moreover, while “[p]redatory pricing is very unlikely on public blockchains,” private blockchains “can change the protocol anytime without having to convince anyone to adopt the change,” and the same goes for pricing.²³³ Similarly, private blockchains can engage in exclusive dealing, that is forming agreements under which customers are obliged to deal with a dominant company.²³⁴ Moreover, discriminatory abuses could easily be encountered on private blockchains, where the records are not necessarily visible.²³⁵

Continuing the doctrinal analysis, the relevant market is not easy to define. In the *Cellophane Case*, the Court announced the rule that “commodities reasonably interchangeable by consumers for the same purposes make up that ‘part of the trade or commerce,’

²²⁶ See *id.* at 308-09.

²²⁷ See Case 27/76, *United Brands v. Comm’n*, 1978 E.C.R. 0207; Case C-7/97; *Oscar Bronner v. Mediaprint Zeitungs und Zeitschriftenverlag*, 1998 E.C.R. I-07791.

²²⁸ Schrepel, *supra* note 9, at 310.

²²⁹ See *United States v. Microsoft*, 253 F.3d 34 (D.C. Cir. 2001).

²³⁰ Schrepel, *supra* note 9, at 307.

²³¹ See *id.* at 313.

²³² *Id.* at 314.

²³³ *Id.* at 316.

²³⁴ See *id.* at 317.

²³⁵ See *id.* at 321.

monopolization of which may be illegal.”²³⁶ Similar formulations based on demand-side substitution are found in the *United Brands* case,²³⁷ but also in the recent European cases of *Facebook*²³⁸ and *Google Android*.²³⁹ The question, of course, is in how narrowly the market is defined.²⁴⁰ In blockchains used for trade of a single cryptocurrency, e.g., Bitcoin, we could narrow down the relevant market to either the specific coin or all of them. For novel blockchains, used for a variety of applications and tokens, including tokenized tangible goods or non-fungible tokens (NFTs), such as Ethereum, the challenge seems even more pressing.²⁴¹ Since blockchains operate transnationally, the geographic market would presumably always be global, which makes successful claims even more difficult to make out. Perhaps these questions will be answered in *In re Tether* litigation, where the plaintiffs posited a Section 2 monopolization claim, based on inter alia, allegation of artificially manipulated prices of certain cryptocurrencies to deceive the investors.²⁴² The court found the claims plausible and the litigation is ongoing.²⁴³

As we have seen “refusal to grant general access is an essential characteristic of *private* [permissioned] blockchains,” where users “restrict who can enter and who can create smart contracts.”²⁴⁴ Indeed, the “potential for abuse grows considerably if a private blockchain becomes truly essential,” i.e., if the entrance to the blockchain becomes essential to enter a market.²⁴⁵ The gatekeepers “will surely” attempt to

²³⁶ *United States v. E. I. du Pont de Nemours & Co.*, 351 U.S. 377, 395 (1956).

²³⁷ Case C-7/97, *Oscar Bronner v. Mediaprint Zeitungen und Zeitschriftenverlag*, 1998 E.C.R. I-07791.

²³⁸ Case C-252/21, *Meta Platforms Inc., Meta Platforms Inc. Ireland Ltd., Facebook Deutschland GmbH v. Bundeskartellamt*, 2022 E.C.R. 00000.

²³⁹ Case T-612/17, *Google & Alphabet v. Comm’n (Google Shopping)* ECLI:EU:T:2021:763 (Nov. 10, 2021).

²⁴⁰ *See, e.g., Int’l Boxing Club of N.Y. v. United States*, 358 U.S. 242, 262 (1959); *Affiliated Music Enter. v. Sesac, Inc.*, 268 F.2d 13 (2d Cir. 1959).

²⁴¹ SCHREPEL, *supra* note 33, at 185.

²⁴² *In re Tether & Bitfinex Crypto Asset Litig.*, 576 F. Supp. 3d 55, 70 (S.D.N.Y. 2021). *See also* *Lamartine Pierre v. Apple Inc.*, 23-cv-05981-VC, (N.D. Cal. Mar. 26, 2024) (LEXIS) (order granting motion to dismiss). In *Pierre v. Apple*, the court dismissed a blockchain antitrust lawsuit, finding the plaintiffs lacked antitrust standing, failed to define relevant market, and failed to adequately allege an agreement. *Id.* at *1.

²⁴³ *Id.*

²⁴⁴ Schrepel, *supra* note 9, at 310 (alteration added).

²⁴⁵ Treacy & Latham, *supra* note 113, at 607.

eliminate competition in the downstream market in this way.²⁴⁶ Even though the duty to deal doctrine, controversial as it is,²⁴⁷ had been narrowed down in *Verizon v. Trinko*,²⁴⁸ today there is some attempt to revive it to challenge digital platforms.²⁴⁹ Analogous provisions exist in European law.²⁵⁰ It is thus interesting whether a refusal to deal or the essential facilities doctrine could be applied to blockchains. These questions were brought up in the questionable suits of Ryan Gallagher.²⁵¹ While the actions were dismissed, we know that “[t]he high value that we have placed on the right to refuse to deal with other firms does not mean that the right is unqualified.”²⁵² Yet, the definition of the market, the dominant position, and of the essential nature of the platform provided an unsurmountable burden to the plaintiff.²⁵³

Finally, we should underline that the distinction is between the market where a specific blockchain is traded, i.e., where the technology operates as a product or service, and the markets where the tokens (or tokenized products or services) are traded.²⁵⁴ Authors submit that while a blockchain can, theoretically, become a dominant technology, it is more likely it will be used to collude irrespectively of its market power.²⁵⁵ It thus seems that monopolistic abuses may happen on

²⁴⁶ SCHREPEL, *supra* note 33, at 196.

²⁴⁷ *Byars v. Bluff City News Co.*, 609 F.2d 843, 846 (6th Cir. 1980) (whether “a monopolist ha[s] a duty to deal” is “one of the most unsettled and vexatious [issues] in the antitrust field”).

²⁴⁸ *Verizon Commc’ns, Inc. v. L. Offs. of Curtis V. Trinko, LLP*, 540 U.S. 398 (2004).

²⁴⁹ See Erik Hovenkamp, *The Antitrust Duty to Deal in the Age of Big Tech*, 131 *YALE L.J.* 1483 (2022).

²⁵⁰ See *Joined Cases 6 & 7-73, Istituto Chemioterapico Italiano S.p.A. & Com. Solvents Corp. v. Comm’n*, 1974 E.C.R. 1974-00223.

²⁵¹ *Gallagher v. Bitcointalk.org*, No. 18-CV-05892, 2018 WL 7569334 (N.D. Cal. Nov. 27, 2018), *report and recommendation adopted*, No. 18-CV-05892-EMC, 2019 WL 1095799 (N.D. Cal. Jan. 2, 2019).

²⁵² See *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585, 601 (1985); *Verizon Commc’n, Inc. v. Law Off. of Curtis V. Trinko, LLP*, 540 U.S. 398, 408 (2004).

²⁵³ Thibault Schrepel, *The First Case of “Blockchain Antitrust”: Gallagher v. Bitcointalk.org*, *NETWORK LAW REVIEW* (May 28, 2020), <https://www.networklaw-review.org/first-case-blockchain-antitrust/>.

²⁵⁴ Maggiolino & Zoboli, *supra* note 90, at 5.

²⁵⁵ *Id.* at 9 (adding that a dominant blockchain is “far to come”). *But see Blockchain Technology and Competition Policy - Issues paper by the Secretariat*, OCEDE (April 26, 2018) (“Cryptocurrencies that are built on blockchains are likely to be subject to both network and platform effects. Therefore, if in the more distant future

private blockchains, while the scope for collusion may exist on both private and public ledgers.

F. Antitrust Self-Regulation

Evan Miller wrote that “[b]lockchain is not the death of anti-trust.”²⁵⁶ According to Miller, blockchain is supposed to launch an era where antitrust self-regulation, i.e., private ordering measures preventing one or small groups of competitors from monopolizing a market or engaging in otherwise anticompetitive conduct, together with transparency brought by the technology and public voting, bring novel legal problems and a new antitrust paradigm.²⁵⁷ We could see, for example, self-limitation proposals, where the majority of network participants would attempt to prevent the emergence of monopolies or concentrated pools, and thus to preserve the decentralization of the network.²⁵⁸

This concept may remind the reader of *competition by design*, which has recently been gaining traction in the context of algorithmic collusion,²⁵⁹ especially in the EU.²⁶⁰ Outlining this approach, the EU Competition Commissioner, Margrethe Vestager, proclaimed that “[w]hat businesses can—and must—do is to ensure antitrust compliance by design. That means pricing algorithms need to be built in a way that doesn’t allow them to collude.”²⁶¹ The parallel is, however,

they do replace credit card companies, then one or two might gain market power not necessarily because their product is particularly different from another cryptocurrency, but as a result of the take-up of that product by other users.”).

²⁵⁶ Evan Miller, *Antitrust Live: The New Blockchain Era of Antitrust*, 24 COLUM. SCI. & TECH. L. REV. 106, 107 (2022) [hereinafter Miller, *Antitrust Live*] (discussing that blockchain isn’t the death of antitrust).

²⁵⁷ *Id.*

²⁵⁸ *Id.* at 117.

²⁵⁹ See generally Ariel Ezrachi & Maurice E. Stucke, *Artificial Intelligence & Collusion: When Computers Inhibit Competition*, 2017 U. ILL. L. REV. 1775, 1788 (2017) (discussing “algorithmic monopoly” as a form of algorithmic collusion); ARIEL EZRACHI & MAURICE E. STUCKE, *VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY* (2016).

²⁶⁰ Simonetta Vezzoso, *Competition by Design*, in *COMPETITION LAW FOR THE DIGITAL ECONOMY* 93, 114-18 (2019).

²⁶¹ *Id.* at 99 (quoting Margrethe Vestager, *Algorithms and Competition*, Speech at the Bundeskartellamt 18th Conference on Competition, Berlin (Mar. 16, 2017), https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/bundeskartellamt-18thconference-competition-berlin-16-march-2017_en

only superficial. Competition by design relates to algorithms, i.e., objects of property that corporations are liable for anyway, and thus is nothing more than a regulatory mandate to implement precautions within a firm to refrain from activity which is probably illegal. The self-governance we may observe on blockchains differs fundamentally. It is not a unilateral but a joint-self limitation,²⁶² pertaining not to the operation of a firm, but to regulation of the blockchain (i.e., of the community), where some market participants are restrained by other market participants; although the restraint is supposed to promote decentralization, it amounts to an anticompetitive practice in itself.²⁶³

Thus, on the one hand, these measures attempt to achieve the same goals that the law does—on the other, “if adopted, such rules likely would constitute per se violations of those same antitrust laws by artificially limiting competition.”²⁶⁴ This is because these measures attempt to preclude what the law does not: the possession of a monopoly, or a contract in restraint of trade, neither of which is unlawful per se, whether under the Sherman Act or the TFEU, but become wrongs only if coupled with an abusive element.²⁶⁵ Thus, the doctrinal difficulty is twofold. Firstly, the code can embody hard rules (e.g., an *ex ante* limitation of size, i.e., a prevention of access to the ledger) which are not flexible enough to determine whether an act in question is anticompetitive.²⁶⁶ Secondly, and more importantly, if some market

[https://web.archive.org/web/20191129221650/https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/bundeskartellamt-18th-conference-competition-berlin-16-march-2017_en]).

²⁶² *Id.* at 119; see also Coase, *supra* note 96.

²⁶³ Miller, *Antitrust Live*, *supra* note 256, at 117-22.

²⁶⁴ *Id.* (Miller calls this the era of “Antitrust Live”).

²⁶⁵ For the American position, see, e.g., *United States v. Grinnel Corp.*, 384 U.S. 563, 570-71 (1966); *United States v. Aluminum Co. of Am.*, 148 F.2d 416, 430 (2d Cir. 1945); *Byars v. Bluff City News Co., Inc.*, 609 F.2d 843, 853 (6th Cir. 1979). For the European position, see *Case C-209/10, Post Danmark A/S v. Konkurrencerådet*, ECLI:EU:C:2012:172, ¶ 21 (Mar. 27, 2012) (“It is in no way the purpose of Article 82 EC to prevent an undertaking from acquiring, on its own merits, the dominant position on a market . . . [n]or does that provision seek to ensure that competitors less efficient than the undertaking with the dominant position should remain on the market”); *Case C-413/14, Intel Corp. Inc. v. Eur. Comm’n*, ECLI:EU:C:2017:632 (Sep. 6, 2017).

²⁶⁶ Deirdre K. Mulligan & Kenneth A. Bamberger, *Saving Governance-By-Design*, 106 CALIF. L. REV. 697, 704 (2018) (“[G]overnance-by-design overreaches by using overbroad technological fixes that lack the flexibility to balance equities and adapt to changing circumstances.”).

participants are concerned about collusive or monopolistic practices of a firm and decide to conduct a fork to exclude the competitive wrongdoer, the legal legitimacy of such accounting would be null, given it did not come from a state court or agency. In this way, self-limitation would most likely be considered an agreement which unreasonably restrains trade *per se*,²⁶⁷ with any difficulty being evidentiary rather than conceptual. The skeptic would be inclined to apply the *per se* treatment of such self-regulatory activity. However, Miller also argues for doctrinal refinement, given the pro-competitive potential of blockchains and the genuine novelty of the technology. Instead, refining the rule of reason approach to those arrangements would be preferable.²⁶⁸

Going beyond the doctrinal reflection of antitrust, it is interesting whether we could see, for the first time, an emergence of private ordering of antitrust. Until now, self-regulation in the antitrust context was spoken of in relation to internet platforms, which emerged as a result of similar faith in community governance, private ordering, and the creation of efficient self-governing spaces of exchange.²⁶⁹ Similarly, platforms play the role of facilitating transactions; they are “market makers,” setting the rules for participants.²⁷⁰ However, it is the multisided nature of platforms which prevented them from the ordering of antitrust norms: they did not need to prevent a seller from becoming a monopolist and were unconcerned with a seller’s attempts of collusive behavior.²⁷¹ The matters look different on blockchains. We could see, for example, the use of a hard fork of a majority of users to *protect* competitive process, while raising doubts about the legal legitimacy of the action (if it qualifies as a collusive agreement, as examined above).²⁷²

In this respect, the antitrust self-governing of blockchain communities is part of a broader problem that private law has with blockchains. For example, mandatory rules of contract can clash with stipulations of smart contracts encoded by the parties; and corporate law, which increasingly needs to deal with DAOs, self-governing entities

²⁶⁷ 15 U.S.C. § 1; Miller, *Antitrust Live*, *supra* note 256, at 120.

²⁶⁸ Miller, *Antitrust Live*, *supra* note 256, at 124.

²⁶⁹ Bietti, *supra* note 26, at 165.

²⁷⁰ Bietti, *supra* note 26, at 174-75.

²⁷¹ *See generally* Hovenkamp, *supra* note 19.

²⁷² *See* Miller, *Antitrust Live*, *supra* note 256, at 117-22.

which attempt to evade the local rules of the law of organizations.²⁷³ At the same time, as we will see in Part IV, some form of self-regulatory cooperation of blockchains with law enforcement may be necessary for the law to be able to enforce its rules. The jurisprudentially inclined could ask if this would be the first instance of transnational or pluralist antitrust. More realistically, however, cooperation of blockchains with law enforcement will remove the paradox we encountered in this subsection: it would provide blockchain self-enforcement of antitrust with the legitimacy that the law carries.²⁷⁴

IV. SYNTHESIS

As the jurisprudential adage goes, technology is not neutral and is shaped by regulatory action.²⁷⁵ We have seen that not everything about blockchains is pro-competitive and there remains a need for the law to step in. This relates not just to private blockchains; today, the permissionless infrastructure is controlled by a handful of entities, and so “antitrust can be crucial in restoring blockchain’s decentralization.”²⁷⁶ This part examines how novel the challenges brought by blockchain are and if antitrust will be able to resolve them.

A. The Novelty of Blockchain Challenges

We have applied antitrust doctrine to blockchains, showing that the doctrinal challenges can be tackled by the law, even if novel legal fictions or modifications of existing ones are necessary.²⁷⁷ Indeed, although the technological landscape has changed, the change to permissionless blockchains may structurally be for the better, even if the

²⁷³ See, e.g., Blaszczyk, *Decentralized Autonomous Organizations*, *supra* note 91; Kyung Taek Minn, *Towards Enhanced Oversight of “Self-Governing” Decentralized Autonomous Organizations: Case Study of The DAO and its Shortcomings*, 9 N.Y.U. J. INTELL. PROP. & ENT. L. 139 (2019).

²⁷⁴ Lianos, *supra* note 132, at 91 (writing that competition by design “may [also] be promoted through competition advocacy and a more active informal engagement of competition authorities with the blockchain community so to nudge them to the right direction.”).

²⁷⁵ See LESSIG, *supra* note 2.

²⁷⁶ Massarotto, *supra* note 147, at 121.

²⁷⁷ See Martinez, *supra* note 182, at 497-98 (“[T]o preserve the relevance of antitrust law in DeFi markets as they become increasingly sophisticated, the current state of antitrust law must take care to adapt along with them.”).

platforms of web 2.0 are not replaced by community driven alternatives. It is undeniable that blockchains have the potential to benefit consumers by lowering prices or increasing output: one needs only to see how fast the technology is growing and how widely it becomes adopted. At the same time, the potential for anticompetitive conduct, found mostly on private, permissioned chains, does not present a significant doctrinal difficulty: since permissioned blockchains have a more easily identifiable locus of control, finding of the liable parties will not be too difficult.²⁷⁸ In fact, the technological features of pseudonymity and immutability, which preserve a record of the dealings between parties and allow for cartel facilitation, can similarly be used by the law enforcement to detect violations.²⁷⁹ In fact, some “do not see a conflict between competition law and blockchain, any more than there is a conflict between competition law and email or electricity.”²⁸⁰

At the same time, decentralization and the move towards self-enforcement may be seen as challenging to competition law and policy. This is especially so if we believe, like neo-Brandeisians do, that consumer welfare and the encouragement of creative destruction are not the only ends of antitrust. In this way, Samuel N. Weinstein argues that regulators making blockchain competition policy must also consider whether there can be too much decentralization and weigh the “benefits of increased competition against threats to safety and soundness.”²⁸¹ Indeed, permissionless blockchains can destabilize the role of intermediaries; permissioned blockchains created by big platforms can solidify their position. Finally, blockchains decentralize the process, but not necessarily the outcomes. Power structures emerge, sometimes without an anticompetitive effect, or at least ‘bigness’ in structure.²⁸² Most importantly for our purposes, blockchains create obstacles to effective enforcement of competition law. If the vision of *lex cryptographia* proponents was true, i.e., if the law was unenforceable on public, permissionless blockchains, then we would end up with

²⁷⁸ Weinstein, *supra* note 32, at 508 (writing that the challenges are “not novel and can be addressed using current law and enforcement strategies.”).

²⁷⁹ *Id.* (writing that the “transparency blockchain offers may simplify discovery and prosecution of antitrust violations,” reducing the need to sift through paperwork, while decrypting the identity of offenders is not an unsurmountable challenge either).

²⁸⁰ Pike & Carovano, *supra* note 62, at 108.

²⁸¹ Weinstein, *supra* note 32, at 546.

²⁸² See *supra* note 107.

the antitrust death examined in the beginning of the essay. It seems, however, that the death of antitrust has been proclaimed prematurely.

B. Practical Limitations on Antitrust and Governance by Design

Even with respect to well-known industries, the limits of antitrust are mostly practical, stemming from “choices made more or less consciously by institutions tasked with applying statutes designed to curb monopoly power” to imperfect facts, rather than ideology or theory.²⁸³ The recent *Federal Trade Commission v. Meta Platforms* case proves the point,²⁸⁴ also signaling a divide between the United States’ close-to-reality approach and the probabilistic method of the European Union.²⁸⁵ Blockchain seems to add a further hurdle: it is an immutable, i.e., practically unchangeable and unstoppable code, with many participants of networks preserving pseudonymity.²⁸⁶ Thus, “even if a practice is identified as being anticompetitive, it cannot be deleted or stopped . . . [and] effective ways to apply antitrust law to blockchain are yet to be found.”²⁸⁷ The law requires novel modes of regulatory intervention encoded in the law.²⁸⁸

Indeed, several proposals to this effect have been made. A radical one, evoking the corporatist flair of the once upon a time Roosevelt ideas, comes from Massarotto. She argues that a single universal blockchain should be devised, which would simplify the issues arising in the currently distributed architecture, and create a single universal platform on which goods and services are traded.²⁸⁹ Such universal blockchain would be weaponized—due to the transparency enabled by the technology—by the FTC and the DOJ to tackle the antitrust

²⁸³ Nicolas Petit, *A Theory of Antitrust Limits*, 28 GEO. MASON L. REV. 1399, 1400 (2021).

²⁸⁴ Fed. Trade Comm’n v. Meta Platforms Inc., No. 5:22-CV-04325, 2022 WL 16637996 (N.D. Cal. Nov. 2, 2022).

²⁸⁵ Petit, *supra* note 283, at 1460.

²⁸⁶ Thibault Schrepel, *Collusion by Blockchain and Smart Contracts*, 33 HARV. J.L. & TECH 117, 153 (2019) (“In short, mostly for technical reasons, blockchain greatly complicates the work of antitrust and competition agencies.”).

²⁸⁷ Schrepel, *supra* note 9, at 323-25.

²⁸⁸ *Id.* at 335.

²⁸⁹ Giovanna Massarotto, *From Digital to Blockchain Markets: What Role for Antitrust and Regulation* (Jan. 26, 2019), <https://ssrn.com/abstract=3323420>.

underenforcement.²⁹⁰ Further, to prevent the web 3.0, from being an extension of the currently existing economy, agencies would use blockchains to “tackle forms of monopolization and collusion in quasi-monopoly data driven markets” and even to “prevent some companies that now exert monopoly power in crucial markets from entering into certain blockchain business[es].”²⁹¹ After all, “antitrust and effective forms of regulation are necessary to build—trust.”²⁹² Indeed, according to blockchain’s proponents, “blockchains can complement antitrust law in realms where the latter is inapplicable or underenforced.”²⁹³

For any of this to happen, absent the creation of a single state-governed permissioned chain, a regulatory entry point must be established. According to Schrepel, the law must be encoded on blockchains.²⁹⁴ Thus, Weinstein proposed that all permissioned financial blockchains would be required to “open a regulatory node through which their assigned oversight agency can actively monitor the network is technologically feasible, and the financial regulators should mandate such access.”²⁹⁵ He further proposed to “require or encourage open blockchain standards and mandate that dominant [permissioned] blockchain networks offer open and non-discriminatory access to users who meet reasonable and fair membership criteria.”²⁹⁶ In fact, the first steps in this direction have been taken in the European Financial Transparency Gateway,²⁹⁷ and we can imagine further projects of the European Single Access Point and the European Blockchain Sandbox to explore it further.²⁹⁸

²⁹⁰ See Giovanna Massarotto, *Can Blockchain Technologies Resolve the U.S. Antitrust Enforcement Problem?*, 25 U. PA. J. BUS. L. 657 (2023).

²⁹¹ Massarotto, *Antitrust in the Blockchain Era*, *supra* note 121, at 267-68.

²⁹² *Id.* at 274. (italics omitted)

²⁹³ Schrepel & Buterin, *supra* note 39, at 3.

²⁹⁴ Schrepel, *supra* note 9, at 335.

²⁹⁵ Weinstein, *supra* note 32, at 554.

²⁹⁶ *Id.* at 515.

²⁹⁷ See Davilla, *supra* note 154; European Financial Transparency Gateway (2020), https://finance.ec.europa.eu/system/files/2020-03/finance-200401-digital-finance-coding-challenge-eftg_en.pdf.

²⁹⁸ Financial transparency – single EU access point for company information, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12776-Financial-transparency-single-EU-access-point-for-company-information_en; European Blockchain Sandbox: Best Practices Report, EUROPEAN COMMISSION (2023), <https://digital-strategy.ec.europa.eu/en/library/european-blockchain-sandbox-best-practices-report>.

The debate around finding the technical means of exercising antitrust oversight over distributed ledgers, a backdoor allowing competition authorities and the courts for enforcement, is reminiscent of the “key escrow” proposal from the days of the previous cryptographic revolution; a precedent which is rather unpromising. Worried that encryption technology would impair the ability of law enforcement to tackle illegal activities, the Clinton administration proposed that special data recovery keys be used, which would enable backup decryption by government officials authorized to access this information.²⁹⁹ Those backdoors were to be implemented through a voluntary use of a device called “Clipper Chip” and, as the reader may guess from the anachronistic name, it largely failed, and so did the later “software key escrow” proposal, mainly due to privacy, civil liberties, and government spending concerns.³⁰⁰ There were also fundamental practical difficulties with securing a database of end-user keys.³⁰¹ Most importantly, however, the implementation of this solution would have stifled economic and technological progress, imposing additional costs on the easy and cheap use of technology.³⁰² The same story could repeat itself in relation to blockchains, with further concerns over the constitutionality of the solution, should the backdoors be mandatory.³⁰³

Another solution, however, lies in utilizing the private ordering potential of the technology and engaging in cooperation between the law and blockchain communities.³⁰⁴ The developers and users of blockchains should be incentivized to facilitate legal enforcement,

²⁹⁹ Dorothy E. Denning & William E. Baugh, Jr., *Key Escrow Encryption Policies and Technologies*, 41 VILL. L. REV. 289 (1996) (citing White House Press Release, Statement of the Press Secretary, Apr. 16, 1993, 1993 WL 357773).

³⁰⁰ Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1063 (2014); A. Michael Froomkin, *It Came from Planet Clipper: The Battle Over Cryptographic Key “Escrow”*, 1996 U. CHI. LEGAL F. 15, 24 (1996) (“[T]he strategy failed when the public refused to buy or use the product.”). See also Steven Levy, *Why Are We Fighting the Crypto Wars Again?*, WIRED (Mar. 11, 2016, 12:00 AM), <https://www.wired.com/2016/03/why-are-we-fighting-the-crypto-wars-again>.

³⁰¹ Matt Blaze, *Key Escrow From a Safe Distance*, 317 ACSAC ‘11 (Dec. 5-9, 2011), <https://dl.acm.org/doi/pdf/10.1145/2076732.2076777>, at 321.

³⁰² *Id.*

³⁰³ See also A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995). But see Anjali Singhal, *The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography*, 7 STAN. L. & POL’Y REV. 189, 200 (1996).

³⁰⁴ See Lianos, *supra* note 132, at 91.

integrating the law and code.³⁰⁵ In this way, rather than resort to a key escrow, the law would utilize the very features of the technology which make it problematic—the unstoppable code, which makes each blockchain akin to a fortress and is a regulatory modality similar to the law itself.³⁰⁶ Thus, developers could encode the law into the protocols themselves.³⁰⁷ In this way, a regulatory cooperation of communities self-enforcing antitrust laws or doing so under the regulators’ guidance would emerge.³⁰⁸ It should be apparent that this cooperation lends institutional legitimacy to private ordering measures which, rather than violate antitrust norms, will now be coopted to enforce it. This cooperation can be incentivized, most straightforwardly, through the threat of imposition of costs, i.e., making legally non-compliant blockchains illegal, moving the rule of law downstream, for example, tackling cryptocurrency exchanges, internet services providers, or identifiable developers.³⁰⁹ Other methods include promoting antitrust law-compliant blockchains through safe harbors and regulatory sandboxes.³¹⁰

Finally, it seems that the further we move towards employing computational, predictive methods in antitrust, that is, using artificial intelligence to predict the likelihood of antitrust harm occurrence, the more appealing the law-as-code approach sounds.³¹¹ Indeed, combining computational methods with blockchain and smart contracts may not only respond to the technological challenge, but also have a transformative effect, potentially translating into computer code not only rules, injunctions, and decrees, further automatizing companies’ compliance with antitrust rules.³¹² Indeed, the Department of Justice and sixty-five antitrust agencies have joined the pioneering computational antitrust project,³¹³ researching the possibility of using new

³⁰⁵ SCHREPEL, *supra* note 33, at 232.

³⁰⁶ *Id.* at 239. *See also* LESSIG, *supra* note 2.

³⁰⁷ SCHREPEL, *supra* note 33, at 241.

³⁰⁸ *Id.*

³⁰⁹ *See* Lianos, *supra* note 132, at 90 (“Individual sanctions may constitute the best option, for instance imposing a fine to the core developers.”)

³¹⁰ Buterin & Schrepel, *supra* note 39, at 11.

³¹¹ *See* SCHREPEL, *supra* note 33, at 250 (outlining “futarchic” antitrust); John McCaskill, Euel Elliott, James Harrington, & L. Douglas Kiel, *Antitrust Policy and Blockchain Technology: An Exploration from the Complex Systems Perspective*, 2 STAN. COMPUTATIONAL ANTITRUST 117 (2020).

³¹² Massarotto, *Can Antitrust Trust Blockchain?*, *supra* note 147, at 135.

³¹³ Press Release 21-72, Office of Public Affairs U.S. Department of Justice, Justice Department Joins Computational Antitrust Project at Stanford Law School, 21-

enforcement methods,³¹⁴ while the authorities of the International Competition Network, including the FTC, have announced plans to increase their technological capacity.³¹⁵ In this way, we may achieve the blockchain antitrust synthesis.

V. CONCLUSION

Blockchain offers a challenge to digital gatekeepers and to antitrust doctrine and theory alike. The technology carries the potential to realize the goals of competition law, starting with lowering of prices and increasing outputs, further addressing “bigness” worries, and finally offering a promise of an economy of peers. As always, the ideals appear more attractive than the reality³¹⁶ and antitrust law must confront anticompetitive practices, not only on permissioned blockchains where they may proliferate, but possibly also on permissionless ledgers. At the same time, the skeptical case has been overstated; most of the challenges are, in fact, routine. The novel ones, such as the possibility of community-based private ordering of antitrust, the testing of conceptual limits, and a challenge to enforcement are yet another nudge towards flexibility and enforcement modernization, for example through antitrust by design or computational competition law, and facilitating the innovative, and pro-competitive architecture of blockchains.³¹⁷ What of antitrust’s supposed death? *Le roi est mort, vive le roi!*³¹⁸

72 (Jan. 19, 2021), <https://www.justice.gov/opa/pr/justice-department-joins-computational-antitrust-project-stanford-law-school>.

³¹⁴ See Herwig C.H. Hofmann & Isabella Lorenzoni, *Future Challenges for Automation in Competition Law Enforcement*, 3 STAN. COMPUTATIONAL ANTITRUST 36 (2023). See also Cary Coglianese & Alicia Lai, *Antitrust by Algorithm*, 2 STAN. COMPUTATIONAL ANTITRUST 1 (2022).

³¹⁵ *Building Digital Capacity to Strengthen and Support Law Enforcement Agencies*, INT’L COMPETITION NETWORK (Mar. 26, 2024), <https://www.internationalcompetitionnetwork.org/working-groups/icn-operations/technologists/technologist-forum-statement-on-building-agency-digital-capacity/>; *Building Tech Capacity in Law Enforcement Agencies*, FED. TRADE COMM’N (Mar. 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/ot.techcapacityreport.pdf.

³¹⁶ See SØREN KIERKEGAARD, EITHER/OR PART I 41 (Howard V. Hong & Edna H. Hong eds., 1987) (“Pleasure disappoints; possibility does not”).

³¹⁷ See Lianos, *supra* note 132, at 47 (calling this a Schumpeterian paradigm of regulation).

³¹⁸ “The king is dead, long live the king!” (translated from French).