
The Journal of the
Antitrust, UCL and Privacy Section
of the California Lawyers Association

TABLE OF CONTENTS

<u>Articles</u>	<u>Page</u>
AI AND INTERDEPENDENT PRICING: COMBINATION WITHOUT CONSPIRACY? Joshua P. Davis and Anupama K. Reddy	1
BLOCKCHAIN TECHNOLOGY: A FUTURE ANTITRUST TARGET? Ryan C. Thomas and Peter Julian	18
BIG DATA AND ANTITRUST RISKS IN CLOSE-UP: FROM THE PERSPECTIVE OF REAL CASES Ken Dai and Jet Deng	36
DIGITAL PLATFORM COMPETITION, MERGER CONTROL, AND THE INCENTIVE TO INNOVATE: DON'T KILL THE GOOSE THAT LAYS THE GOLDEN EGG John Ceccio and Christopher Mufarrige.....	52
IT'S HIGH TIDE AGAIN IN INTERNET MARKETS Josh Palmer.....	70
THE SIMPLE ECONOMICS OF HYBRID MARKETPLACES Neil Dryden, Sergey Khodjamirian, and Jorge Padilla	85
PRIVACY, PRICING, AND THE VALUE OF CONSUMER DATA: THE COMPLEX NATURE OF THE CCPA'S NON-DISCRIMINATION REQUIREMENT Jeewon Kim Serrato and Lawrence Wu.....	100
THE FTAIA'S "DOMESTIC EFFECTS" EXCEPTION: WHY THE NINTH CIRCUIT GOT IT RIGHT Stephen McIntyre.....	113
FOURTH ANNUAL "CELEBRATING WOMEN IN COMPETITION LAW IN CALIFORNIA"	127

BLOCKCHAIN TECHNOLOGY: A FUTURE ANTITRUST TARGET?

By Ryan C. Thomas and Peter Julian¹

I. INTRODUCTION

Technology companies face increasing antitrust scrutiny globally. In the United States, lawmakers are ramping up pressure to increase enforcement at federal and state levels. Several high-profile politicians, including U.S. presidential candidates, have called for new antitrust legislation that would make it easier to pursue allegedly “dominant” companies, especially leading technology firms.² As more companies rebrand themselves to embrace e-commerce, future antitrust enforcement and private suits will extend beyond the large online platforms.

As blockchain applications increasingly expand beyond cryptocurrency into other areas, including supply chain and government bidding, companies and competition enforcers are developing experience with how antitrust issues play out with this much-hyped technology. Meanwhile, initial concerns around prematurely regulating and potentially stifling this emerging technology have given way to legislative efforts to limit illicit cryptocurrency uses, while promoting lawful uses of blockchain technology. While the promise of a sweeping blockchain revolution across the economy may seem overstated, real-world implementations have been progressing. This article explores the antitrust issues presented by blockchain implementations and implications for companies considering adopting blockchain technology.

Blockchain technology (or distributed ledger technology—the two are used interchangeably throughout this article) was first conceptualized in 2008 for use in Bitcoin.³ Since then, the technology and “use cases” (applications) continue to evolve. Although by no means ubiquitous, every year more companies, including established, sophisticated players, are entering the blockchain “market.”⁴ Investors are still paying attention to and pouring significant sums of money into blockchain startups, and businesses are actively

1 Ryan C. Thomas is a partner in the Washington, DC office of Jones Day. Peter Julian is an associate in the firm’s San Francisco office. The authors wish to recognize and thank Jones Day summer associate and UC Hastings College of Law student Amul Kalia for his valuable contributions to this article. The views and opinions set forth herein are the personal views or opinions of the authors; they do not necessarily reflect views or opinions of Jones Day.

2 There is significant disagreement about whether regulatory intervention is necessary at all, or what regulation is warranted. *See, e.g.*, Makan Delrahim, Assistant Attorney General for the U.S. Department of Justice Antitrust Division, Keynote Address at Silicon Flatirons Annual Technology Policy Conference, <https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-keynote-address-silicon-flatirons> (cautioning against “misplaced” and “extreme views” that propose new rules to regulate online platforms and displace the “consumer welfare” standard in antitrust reviews).

3 *Blockchains: The great chain of being sure about things*, THE ECONOMIST (Oct. 31, 2015), <https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things>.

4 *See infra* notes 9–12 and accompanying text.

implementing the technology.⁵ “Platform” blockchains and blockchain as a service (BaaS) are becoming more common, making it easier for businesses to use the technology. Instead of having to code a proprietary blockchain solution from the ground-up, which can be a complicated and expensive endeavor, businesses can use open source solutions, such as Hyperledger,⁶ Enterprise Ethereum,⁷ or R3’s Corda,⁸ adapted to their particular application. In addition, leading enterprise software companies like IBM,⁹ SAP,¹⁰ and Oracle¹¹ have begun offering BaaS that make it even easier for businesses to explore and deploy the technology.¹² These developments have given rise to increasing emphasis on standardization and interoperability between blockchain networks to prevent data silos.¹³

Blockchain also continues to attract significant regulatory and legislative attention based on its disruptive potential. The acting United States Comptroller of the Currency (a former general counsel of a major cryptocurrency exchange)¹⁴ recently issued rulemaking notices aimed at proliferating the use of both cryptocurrency and blockchain technology within the banking sector.¹⁵ The rulemaking notice specifically seeks input on how blockchain technology is used or potentially could be used in the banking industry.¹⁶

Apart from potential agency rulemaking, legislators at both the federal and state levels are introducing bills aimed at providing a regulatory framework for the use of blockchain and cryptocurrencies.¹⁷ At the federal level, the 116th Congress recently issued more than thirty-two such bills. The bills address a number of topics, such as limiting the use of cryptocurrencies for potential terrorism, sex trafficking, and money laundering, while

5 *Deloitte’s 2020 Global Blockchain Survey: From Promise to Reality*, Deloitte, https://www2.deloitte.com/content/dam/insights/us/articles/6608_2020-global-blockchain-survey/DI_CIR%202020%20global%20blockchain%20survey.pdf. (According to the survey, 39% of 1,488 senior executives and practitioners in fourteen countries said they have already incorporated blockchain into production at their companies—a 16% increase from 2019).

6 *About Hyperledger*, Hyperledger, <https://www.hyperledger.org/about>.

7 *About Enterprise Ethereum Alliance*, Enterprise Ethereum, <https://entethalliance.org>.

8 *About R3*, R3, <https://www.r3.com/about>.

9 *IBM Blockchain Solutions*, IBM, <https://www.ibm.com/blockchain/solutions>.

10 *Blockchain Applications and Services*, SAP, <https://www.sap.com/products/intelligent-technologies/blockchain.html>.

11 *Oracle Blockchain*, Oracle, <https://www.oracle.com/blockchain>.

12 Lucas Mearian, *Gartner: Blockchain Will be Nothing More than an Add-on for ERP, CRM Software*, Computerworld (Sept. 16, 2019), <https://www.computerworld.com/article/3438838/gartner-blockchain-will-be-nothing-more-than-an-add-on-for-erp-crm-software.html>.

13 See, e.g., *Building an Interoperable Blockchain-enabled Ecosystem*, HIMSS (May 11, 2020), <https://www.himsslearn.org/building-interoperable-blockchain-enabled-ecosystem>.

14 Cory Johnson, *Trump’s New Top Banking Regulator is a Bitcoin Bull*, FORBES (June 11, 2020), <https://www.forbes.com/sites/coryjohnson/2020/06/11/trump-regulator-bitcoin-bull>.

15 *OCC Requests Comment on Proposal to Update Activities and Operations Rules and its Rules on Digital Activities*, Office of the Comptroller of the Currency (June 4, 2020), <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-76.html>.

16 *Id.*

17 This article is primarily concerned with blockchains, and not cryptocurrencies. The latter is an implementation of blockchain technology, but the two terms are often used interchangeably and have come to be closely associated in the zeitgeist.

promoting a working group to study the use of blockchain technology.¹⁸ States are also jumping into the fray. In 2019, twenty-eight states introduced bills aimed at regulating the blockchain and cryptocurrency space, with a majority of them signed and enacted.¹⁹ As these developments illustrate, legislative and regulatory bodies are concerned with blockchain and cryptocurrency's implications for the future, and are taking measures to promote their lawful use. Early concerns around burdening a new technology with regulations that may stunt its potential are giving way to a wave of new regulations aimed at both regulating and fostering its growth.²⁰

Antitrust authorities are paying attention, too. As recently as August 27, 2020, the head of the Department of Justice Antitrust Division, Assistant Attorney General Makan Delrahim, confirmed that the Division was studying the competitive effects of blockchain technology.²¹ The Division has implemented a program where government attorneys and economists are taking an online course to “build [their] expertise . . . in cutting edge business applications: specifically, blockchain” and other technologies with the goal of “develop[ing] a basic but critical understanding of how businesses implement these technologies and what effect they might have on competition.”²² Delrahim acknowledged that while the technology does have the potential to increase efficiencies, for example, in the financial technology sector, it also has the potential to lead to cartel-like behavior, and stated “the Division will play a critical role in ensuring market conditions are conducive to unleashing blockchain’s revolutionary potential.”²³ DOJ is not alone.

-
- 18 Jason Brett, *Congress Has Now Introduced 32 Crypto and Blockchain Bills*, FORBES (Apr. 8, 2020), <https://www.forbes.com/sites/jasonbrett/2020/04/28/congress-has-introduced-32-crypto-and-blockchain-bills-for-consideration-in-2019-2020>.
- 19 Heather Morton, *Blockchain 2019 Legislation*, National Conference of State Legislatures (July 23, 2019), <https://www.ncsl.org/research/financial-services-and-commerce/blockchain-2019-legislation.aspx>.
- 20 Concerns regarding onerous regulations were most prominently raised during the debate surrounding the passage of New York’s BitLicense regime. See *Stop BitLicense from harming small businesses and tech innovation in NY*, Change.org, <https://www.change.org/p/governor-andrew-m-cuomo-and-the-new-york-state-legislature-stop-bitlicense-from-harming-small-businesses-and-tech-innovation-in-ny>.
- 21 See Makan Delrahim, Assistant Attorney General, Antitrust Division, U.S. Department of Justice, *Assistant Attorney General Makan Delrahim Delivers Remarks at the Thirteenth Annual Conference on Innovation Economics* (Aug. 27, 2020), <https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-thirteenth-annual-conference>; see also *GAI Discussion Series: Assistant Attorney General Makan Delrahim & Judge Douglas H. Ginsburg*, George Mason University - Antonin Scalia School of Law, Global Antitrust Institute Online Discussion Series (June 16, 2020), <https://www.youtube.com/watch?v=YRvV6jo2f-I>.
- 22 *Id.* While controversial, the DOJ has previously opened investigations to learn more about new segments, even when it allegedly had no competitive concerns. See letter from Makan Delrahim, Ass’t Att’y Gen., Antitrust Division, U.S. Dep’t of Justice, to Jerrold Nadler, U.S.H.R. (July 1, 2020), available at <https://www.politico.com/f/?id=00000173-0d14-dd78-a9ff-7fb6e2a70000> (“As the Division was deciding whether to open a[] [merger] investigation, it faced significant matters of first impression regarding the role of antitrust in this industry. . . . Without sufficient information to resolve a competition concern or understand what the likely effects of the merger may be, it is appropriate for the Division to investigate further.”).
- 23 Delrahim, *supra* note 21.

Other competition authorities are paying close attention to the technology as it gets deployed more widely. In February 2018, the European Commission announced the “EU Blockchain Observatory and Forum.”²⁴ In March 2018, the Federal Trade Commission announced the creation of an internal “FTC Blockchain Working Group.”²⁵ Soon after, in April 2018, the Organization for Economic Cooperation and Development published an issues paper titled, “Blockchain Technology and Competition Policy.”²⁶ The movement by government agencies to better understand blockchain increases the likelihood of scrutiny and potential enforcement actions, and businesses are well advised to evaluate the antitrust risks associated with deploying the technology.

While the rollout of blockchain is by no means ubiquitous, the technology is finding its audience and use cases. We will explore a few examples in this article, analyzing potential antitrust implications for other applications. First, we begin with a short overview of distributed ledger technology. Then, we discuss potential antitrust issues, with an emphasis on U.S. competition law. Finally, we discuss a few prominent contemporary examples of blockchain technology implementation and lessons learned for future adaptations.

II. BLOCKCHAIN BASICS

A full discussion about the mechanics of blockchain technology is outside the scope of this article. We address below a few crucial characteristics that will be helpful in discussing the antitrust implications. At its core, a blockchain is a shared ledger in which transactions are recorded and stored in a verifiable way.²⁷ Records of transactions are stored along with other transactions into “blocks” of data that are linked to one another in a “chain.”²⁸ The ledger or database is hosted by a number of different users or “nodes.”²⁹ Unlike a traditional database, the ledger does not allow users to delete data or modify existing data—users can only add new transactions to the end of it, much like a ledger recording financial transactions.³⁰ Also, unlike traditional databases in which one central authority controls what information can be accessed or added to the database, a blockchain is distributed across multiple computers in a network (“nodes” in blockchain parlance), each of which can read from or append to the ledger—all while ensuring that every node has an identical copy of the ledger.³¹

24 *European Commission launches the EU Blockchain Observatory and Forum*, European Commission (Feb. 1, 2018), <https://ec.europa.eu/digital-single-market/en/news/european-commission-launches-eu-blockchain-observatory-and-forum>.

25 *It's Time for a FTC Blockchain Working Group*, Federal Trade Commission (Mar. 16, 2018), <https://www.ftc.gov/news-events/blogs/techftc/2018/03/its-time-ftc-blockchain-working-group>.

26 *Blockchain Technology and Competition Policy*, Organisation for Economic Co-operation and Development (Apr. 26, 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).

27 See generally ABA, *BLOCKCHAIN FOR BUSINESS LAWYERS* (2018); Maryanne Murray, *Blockchain Explained*, Reuters (June 15, 2018), <http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html>.

28 *Id.*

29 *Id.*

30 *Id.*

31 *Id.*

Because blockchain nodes are distributed and have no centralized validation system, there must be a “consensus mechanism” for deciding which block to add at the end of the blockchain if there is a conflict between two or more nodes.³² For example, on the Bitcoin blockchain, the party that is the first to correctly solve a computational puzzle gets to propose the next block to the network and is rewarded with bitcoins.³³ This is called “mining.”³⁴ The nodes on the network signal their acceptance of the proposed block by adding it to their copies of the Bitcoin blockchain after validating that the computational puzzle was solved correctly, that the transactions in the block are valid, and that the Bitcoin in each transaction was not previously spent in another transaction.³⁵ If there is a conflict between different versions of the blockchain, the node that has done the largest amount of computational work to validate transactions is considered to have the accurate record. This is known as a “proof of work” consensus mechanism.³⁶ Apart from access to computing power, and thus being able to mine more, there is no practical likelihood that one participant can be strategically prioritized or given an unfair advantage over another.³⁷

Generally, there are two types of blockchains based on levels of openness and distribution: “permissionless” and “permissioned.”³⁸ A permissionless (or public) blockchain is open to anyone who wants to join—there is no central authority acting as a gatekeeper preventing new entrants from being a part of the blockchain network.³⁹ Without a central authority or clearing house, each node keeps a copy of the entire blockchain and is able to contribute data back to the network.⁴⁰ Participants can remain pseudonymous behind unique user identifiers, but can access the transaction data stored in the blockchain by downloading the software.⁴¹ For example, in a supply chain blockchain, the transaction history can be used to assess if the participant has sufficient funds, capacity, and inventory to complete the requested transaction based on the prior recorded transactions that either have credited or debited the account.⁴²

32 Jake Frankenfield, *Consensus Mechanism (Cryptocurrency)*, Investopedia (Jul. 29, 2020), <https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp>.

33 Cryptocurrencies are perhaps the best-known examples of permissionless blockchains where anyone can join and “mine” for rewards by validating transactions on the blockchain.

34 Jake Frankenfield, *Mining*, Investopedia (May 8, 2018), <https://www.investopedia.com/terms/m/mining.asp>.

35 *Id.*

36 *See* Murray, *supra* note 27.

37 *See* Frankenfield, *supra* note 34.

38 Matthew Beedham, *Here's the Difference Between 'Permissioned' and 'Permissionless' Blockchains*, The Next Web (Nov. 5, 2018), <https://thenextweb.com/hardfork/2018/11/05/permissioned-permissionless-blockchains>.

39 *Id.*

40 *Id.*

41 *Id.*

42 *See* Knut Aliche et al., *Blockchain Technology for Supply Chains—A Must or a Maybe?*, McKinsey & Co. (Sept. 12, 2017), <https://www.mckinsey.com/business-functions/operations/our-insights/blockchain-technology-for-supply-chains-a-must-or-a-maybe>.

Public blockchains are well suited for transactions in which participants need pseudonymity and the ability to transact with an unlimited number of other participants.⁴³ However, some public blockchains, especially older ones, have technical barriers, such as speed, scalability, and storage constraints.⁴⁴ These limitations present impediments for business applications in which multiple transactions need to occur quickly and efficiently.⁴⁵ For example, it can take anywhere from ten minutes to sometimes an entire day to confirm a Bitcoin transaction.⁴⁶ Other public blockchains, such as the Ethereum and Bitcoin Cash blockchain network, have improved on some of these limitations, for example, by processing transactions faster.⁴⁷ Because of the limitations of the public blockchains and the fundamental openness within which they operate, “permissioned” blockchains have been developed to maintain efficiency and to address other use cases.⁴⁸

In a “permissioned” (or private) blockchain, an administrator decides which nodes can join the network—the blockchain can be “open” to the public or only to the nodes that have the administrator’s permission.⁴⁹ Private blockchains are likely to have fewer participants, greater potential for information sharing among participants, and less visibility into transactions from outside the blockchain.⁵⁰ As a consequence, they are the architecture that large companies may most often use to interact with suppliers, customers, or other partners.⁵¹ In this respect, private blockchains lose many of the hallmarks of the original form of the blockchain technology, namely a radically open system in which any user can make verifiable pseudonymous transactions and see a history of all past transactions.⁵²

Private blockchain networks in particular can spawn antitrust concerns, given the potential lack of transparency around competitor interactions. Unlike public blockchains, private distributed ledgers:⁵³

- Have an owner who controls or delegates membership, mining rights and rewards, and maintains the shared ledger, including potentially the right to override, edit, or delete the entries on the blockchain.
- Have an owner or designated participants who are responsible for resolving discrepancies, often outside of a proof-of-work system. For example, the

43 See Beedham, *supra* note 38.

44 *Id.*

45 *Id.*

46 See Steven Buchko, *How Long Do Bitcoin Transactions Take?*, CoinCentral (Dec. 12, 2017), <https://coincentral.com/how-long-do-bitcoin-transfers-take>.

47 See Sean Williams, *Which Cryptocurrencies Have the Fastest Transaction Speeds?*, The Motley Fool (Jan. 14, 2018), <https://www.fool.com/investing/2018/01/14/which-cryptocurrencies-have-the-fastest-transaction.aspx>.

48 See Beedham, *supra* note 38.

49 *Id.*

50 *Id.*

51 *Id.*

52 *Id.*

53 *Id.*; see also Murray, *supra* note 27.

consensus mechanism to validate transactions may be “proof of stake” in which a node’s power to validate a transaction depends on its economic “stake” in the particular blockchain network. The idea is that with a larger stake the node will not approve transactions that would undermine the ledger’s integrity.

- Have a limited membership, often without user anonymity, in which participants can match user identifiers to real-world entities.
- Host data that are not readable or writable by the public; consequently the information exchanged cannot be reviewed by nonmembers who lack access.

These attributes often make private blockchains more attractive for business applications. Private blockchains also can scale significantly better than public blockchains because they can use less computationally intensive consensus mechanisms. Likewise, private blockchains are often better suited for regulated industries that must follow mandated processes, such as “Know Your Customer” anti-money laundering and anti-terrorism regulations that require customers to prove their identity.⁵⁴

III. ANTITRUST BASICS

Blockchain and other emerging technologies, like artificial intelligence and “big data” analytics, are evaluated under the same antitrust laws and analytical framework as “old tech,” like smokestack industries.⁵⁵ In the United States, use of blockchain technology primarily raises potential issues under Sherman Act § 1 (no collusion), Sherman Act § 2 (no monopolization), Federal Trade Commission (FTC) Act § 5 (no unfair competition), and Clayton Act § 7 (no anticompetitive transactions).⁵⁶

In recent years, politicians, competition agencies, and mainstream media in the United States and around the world have devoted significant attention to the question of whether technology companies, and more broadly, “high tech” products or services, should be subject to different antitrust enforcement rules. Although there is not always unanimity across or even within jurisdictions, U.S. leadership at the DOJ and a majority of the FTC Commissioners have made statements suggesting that existing laws are sufficient. In 2019, for example, the head of the DOJ Antitrust Division addressed this directly: “Some have suggested changing the antitrust laws, creating new agencies or even regulating the conduct of some firms . . . it bears repeating that our existent framework is flexible enough to detect harm in any industry and emerging ones.”⁵⁷ In 2018, another DOJ official voiced similar sentiments:

54 See, e.g., Financial Industry Regulatory Authority (FINRA) Rule 2090 (Know Your Customer), <https://www.finra.org/rules-guidance/rulebooks/finra-rules/2090#:~:text=Know%20Your%20Customer,-The%20Rule%20Notices&text=Every%20member%20shall%20use%20reasonable,on%20behalf%20of%20such%20customer.>

55 See BLOCKCHAIN FOR BUSINESS LAWYERS, *supra* note 27.

56 While this article primarily concerns U.S. law, other jurisdictions generally enforce similar prohibitions on collusion, monopolization/abuse of dominance, and transactions that may substantially lessen competition. The discussion here may be relevant for those jurisdictions as well.

57 Diane Craft, *Existing U.S. Antitrust Laws Can Address Tech Monopolies*, DOJ Antitrust Chief Says, REUTERS (Nov. 8, 2019), <https://www.reuters.com/article/us-usa-antitrust-idUSKBN1XI2LS>.

Lately, there has been discussion about whether certain conduct—the use of computer algorithms to set prices, for example—should attract the same level of scrutiny as “traditional” price fixing conduct. To be clear, where competitors agree to restrict competition between them, whether by agreeing to display identical gasoline prices at gas stations on opposite street corners, or by fixing prices using advanced technology like online trading platforms or algorithms, they violate the Sherman Act. The agreement to fix the price is the illegal act; the means through which the agreement is carried out is less important.⁵⁸

This statement directly implicates Sherman Act § 1, which prohibits anticompetitive collusion, such as price fixing, bid rigging, or market allocation.⁵⁹ Depending on how a blockchain is formed and operated, it may also implicate other antitrust laws, including those that prohibit monopolization and anticompetitive transactions. For most blockchain collaborations among rival businesses, however, the greatest practical antitrust risk involves collusion and improper information sharing. Participants might use blockchain technology to facilitate a “naked” agreement to fix prices or allocate markets or customers, or to improperly share competitively sensitive data, which might reduce competition. As the head of the DOJ Antitrust Division recently hypothesized:

There is also, most certainly, potential for abuse. Incumbents could use blockchains anticompetitively to exclude competition. For example, consider seafood harvesters that establish a permissioned blockchain to track food through the supply chain and assure quality and sourcing. If multiple competing harvesters conditioned access to that permissioned blockchain on agreeing to certain prices or output, competition and consumers would suffer tremendous harm.⁶⁰

A. Collusion and Improper Information Sharing—Sherman Act § 1

A § 1 violation requires concerted action (an “agreement”) between two or more firms. Most agreements are reviewed under the rule of reason,⁶¹ which examines whether the agreement’s procompetitive benefits outweigh the likelihood of anticompetitive harm.⁶² Certain other agreements between or among competitors, however, such as fixing prices, allocating markets, and rigging bids, are found to always or almost always

58 Andrew Finch, Principal Deputy Assistant Attorney General, Antitrust Division, U.S. Department of Justice, *Remarks at New York Antitrust in the Financial Sector: Hot Issues & Global Perspectives* (May 2, 2018), <https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-andrew-finch-delivers-remarks-antitrust>.

59 15 U.S.C. § 1.

60 See Delrahim, *supra* note 21.

61 See VII PHILIP AREEDA & HERBERT HOVENKAMP, *ANTITRUST LAW* ¶ 1500, at 431 (3d ed. 2012).

62 *Wuxi Multimedia, Ltd. v. Koninklijke Philips Elecs., N.V.*, No. 04cv1136, 2006 WL 6667002, at *3 (S.D. Cal. Jan. 5, 2006) (quoting *Hairston v. Pac. 10 Conf.*, 101 F.3d 1315, 1319 (9th Cir. 1996)), *aff'd*, 280 F. App'x 968 (Fed. Cir. 2008).

harm competition. Such conduct is presumed unlawful without any inquiry into claimed procompetitive benefits (per se analysis).⁶³

Private blockchains can be procompetitive. Because the participants are known to each other, the arrangement could result in reduced transaction costs, improved connections between nodes, and a more equitable validation of the transactions on the chain. However, the same arrangement may increase antitrust risk, such as when competitively sensitive terms such as price, quantity, and customer-specific features and specifications are shared between competitors. In fact, a private blockchain could facilitate an antitrust violation by providing a method to share the information or to monitor participants to ensure they are following the agreement's terms—i.e., not “cheating” on the arrangement. For example, private blockchains could be used to facilitate a price fixing arrangement, which as noted above is a per se violation of § 1, without regard to actual or claimed procompetitive effects.

Beyond more obviously anticompetitive agreements, blockchain participants could also violate § 1 if they use it to facilitate improper exchanges of competitively sensitive information or to unreasonably exclude rivals' access to the blockchain. Agreements to exchange competitively sensitive information may reduce competition, and the exchange itself also may provide evidence of unlawful coordination. Unlike price fixing or customer/market allocation agreements, however, such exchanges are less likely to be deemed per se unlawful under U.S. law. The conduct is instead evaluated under a “rule of reason” analysis, which requires balancing the anticompetitive harm against the procompetitive benefits of the information exchange.⁶⁴

A number of factors are considered to determine whether an information exchange results in anticompetitive harm:

- Source of the information provided (does it involve actual or potential competitors?);
- Nature of the information exchanged (is it competitively sensitive?);⁶⁵
- Industry structure (is the industry composed of many or few competitors?);⁶⁶

63 *Leegin Creative Leather Prods., Inc. v. PSKS, Inc.*, 551 U.S. 877, 885 (2007); see also *Bus. Elecs. Corp. v. Sharp Elecs. Corp.*, 485 U.S. 717, 723 (1988) (“Certain categories of agreements . . . have been held to be *per se* illegal, dispensing with the need for case-by-case evaluation. We have said that *per se* rules are appropriate only for ‘conduct that is manifestly anticompetitive,’ that is, conduct ‘that would always or almost always tend to restrict competition and decrease output.’” (citations omitted)).

64 See *United States v. U.S. Gypsum Co.*, 438 U.S. 422, 441 (1978).

65 See, e.g., *United States v. Container Corp. of Am.*, 393 U.S. 333, 334–36 (1969); *Todd v. Exxon Corp.*, 275 F.3d 191, 211–13 (2d Cir. 2001); *In re Currency Conversion Fee Antitrust Litig.*, 773 F. Supp. 2d 351, 369 (S.D.N.Y. 2011).

66 See, e.g., *Container Corp. of Am.*, 393 U.S. at 336 (finding 18 firms controlling 90 percent of the market was sufficient concentration to support information-exchange claim); *Sugar Inst., Inc. v. United States*, 297 U.S. 553, 572 (1936) (information-exchange violation involving fifteen companies holding 70–80 percent of the market); *Todd*, 275 F.3d at 199 (finding fourteen companies sharing an 80–90 percent market share sufficient to support data-exchange claim on motion to dismiss).

- Whether there is an anticompetitive effect;⁶⁷ and
- Business rationale (could the legitimate business goals have been achieved with less or no exchange of competitively sensitive information?).

The head of the DOJ Antitrust Division recently noted:

Blockchain solutions might, for instance, facilitate sharing of competitively sensitive information. As Dr. Thibault Schrepel has observed, by virtue of its distributed ledger, the blockchain “turns private information into genuinely public information.” It may be difficult (or impossible) to identify which actors are sharing what information because the blockchain is based on pseudonyms and largely anonymous transactions. This combination of factors could embolden competitors to share more competitively sensitive information through the blockchain than they would otherwise. Moreover, blockchain’s smart contract capabilities could facilitate the design and implementation of anticompetitive agreements⁶⁸

In addition, private blockchain participants also may face § 1 risk if they unreasonably exclude competitors from the blockchain.⁶⁹ If a blockchain were to become critical to compete in a particular industry, competitors may need to be a part of the blockchain. Take costs, for example. Benefits from increased economies of scale (improving cost through greater output of a single good) and scope (improving cost through greater variety of goods) are critical elements of competition in most sectors. In banking and healthcare, for example, using blockchain technology can significantly reduce transactions costs. In healthcare, providers may not be able to provide the same level of care or generate necessary operating efficiencies without access to data on certain blockchain networks or pharmaceutical supply chains. If private blockchain members exclude competitors from accessing a blockchain that has become essential to doing business, nonmembers may not be able to compete effectively. Excluding rivals from a “must have” blockchain may give rise to claims that the blockchain’s membership rules are being used to unfairly exclude or limit competition.

Exclusionary conduct also can result from a blockchain’s architecture—for example, the consensus mechanism chosen to resolve discrepancies. In private blockchains, owners or designated blockchain participants may have the authority to resolve discrepancies in the chain unilaterally, as opposed to a more objective and equitable consensus mechanism. Certain participants could agree to resolve discrepancies against rival competitors and

67 See, e.g., U.S. DEP’T OF JUSTICE & FED. TRADE COMM’N, ANTITRUST GUIDANCE FOR HUMAN RESOURCES PROFESSIONALS 4 (2016) (“While agreements to share information are not per se illegal . . . they may be subject to civil antitrust liability when they have, or are likely to have, an anticompetitive effect.”).

68 See Delrahim, *supra* note 21.

69 See BLOCKCHAIN FOR BUSINESS LAWYERS, *supra* note 27.

to prioritize others.⁷⁰ Although a decision to exclude a competitor from a membership association is typically analyzed under the rule of reason, excluding a rival solely to impede its ability to compete and without a legitimate business justification may be deemed to be anticompetitive conduct.

B. Monopolization—Sherman Act § 2

Sherman Act § 2 generally prohibits monopolization and attempts to monopolize.⁷¹ Importantly, monopoly power alone is not enough to prevail on a Section 2 claim.⁷² Rather, the entity must use its monopoly power to willfully maintain that power through anticompetitive exclusionary or predatory conduct.⁷³ Courts have found exclusionary conduct in a number of circumstances, including, for example, when a monopolist has refused to deal with its rivals, has engaged in exclusive supply or purchase agreements, or has denied an essential facility to its competitors.⁷⁴

The analysis is intensely fact specific, but blockchains may provide evidence of a Section 2 violation if, for example, as part of an exclusive supply arrangement a firm with monopoly power requires its customers to use its blockchain to complete transactions and that requirement results in customers having to abandon a competitor’s blockchain. Section 2 also can be triggered in certain limited circumstances when a monopolist refuses to deal with a competitor. Although a company generally has no duty to deal with its rivals, courts have found antitrust liability when a monopolist had a prior course of dealing with the competitor but then terminated the relationship without any legitimate business reason.⁷⁵ Accordingly, a monopolist owner of a blockchain may face Section 2 scrutiny if it previously allowed a competitor access to its blockchain, but later excluded that rival without a reasonable business justification.

70 *Private Blockchain or Database? How to Determine the Difference*, The Blockchain Review (Oct. 4, 2016), <https://medium.com/blockchain-review/private-blockchain-or-database-whats-the-difference-523e7d42edc> (“[T]he security promises of distributed ledgers and private blockchains are only as good as the honesty of the entities validating the transactions. There are no mathematical guarantees behind the irreversibility of transactions in a private blockchain.”).

71 15 U.S.C. § 2.

72 *United States v. Grinnell Corp.*, 384 U.S. 563, 570–71 (1966); *see also Verizon Commc’ns v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 407 (2004) (“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,” and in order to “safeguard the incentive to innovate, the possession of monopoly power will not be found unlawful unless it is accompanied by an element of anticompetitive *conduct*.”).

73 *See* BLOCKCHAIN FOR BUSINESS LAWYERS, *supra* note 27.

74 *See Trinko, LLP*, 540 U.S. at 407.

75 *See, e.g., Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585 (1985); *Trinko*, 540 U.S. at 407 (“*Aspen* is at or near the outer boundary of § 2 liability . . .”); *see also Viamedia, Inc. v. Comcast Corp.*, 951 F.3d 429, 458 (7th Cir. 2020) (holding refusals to deal may violate the antitrust laws if they involve “withdraw[ing] from a prior course of dealing,” “forgoing short-run profits,” and “treating a rival differently” from others).

C. Unfair Competition—Federal Trade Commission Act § 5

Section 5 of the FTC Act prohibits unfair competition.⁷⁶ The FTC has adopted an expansive and at times controversial interpretation of its enforcement powers under this statute, asserting that Section 5 applies to any “deceptive, collusive, coercive, predatory, unethical, or exclusionary conduct or any course of conduct that causes actual or incipient harm to competition,” including conduct that is not covered by the Sherman Act.⁷⁷ One of the more common applications of Section 5 involves invitations to collude—efforts by one firm to enter into an anticompetitive price fixing or market allocation agreement with one or more of its competitors.⁷⁸

Because blockchains can be used to share information, they could potentially be used to “signal” future plans to rivals and invite them to follow suit. For example, a competitor could use blockchain transaction histories to demonstrate to its competitors that it had been consistently charging a particular price, and then—successfully or unsuccessfully—suggest that they do the same. Or if a blockchain allowed rivals’ access to prospective pricing or other competitively sensitive information, that could be used to signal plans and invite others to follow. Such activity may be viewed as an invitation to collude in violation of Section 5, particularly if there is evidence that competitors’ subsequent transactions and posted prices were impacted by the signal.

D. Anticompetitive Transactions—Clayton Act § 7

Section 7 of the Clayton Act prohibits anticompetitive transactions, including mergers and acquisitions and certain joint ventures and competitor collaborations.⁷⁹ The key question is whether the proposed transaction is likely to create or enhance market power, or to facilitate its exercise.⁸⁰ A transaction is less likely to be anticompetitive if entry or repositioning in the market is easy, or if the merged firm and its remaining rivals could not profitably raise prices or otherwise reduce competition. In addition, when competitive

76 15 U.S.C. § 45.

77 See, e.g., Compl. ¶ 1, *In re Intel Corp.*, FTC Docket No. 9341 (December 16, 2009), <http://www.ftc.gov/os/adjpro/d9341/091216intelcmpt.pdf>; Compl. at 31, *FTC v. Qualcomm Inc.*, No. 5:17-cv-00220, 2017 WL 242848 (N.D. Cal. Jan. 17, 2017), ECF No. 1 (suggesting Section 5 would catch conduct beyond the reach of Sherman Act, § 2: “Qualcomm’s practices, regardless of whether they constitute monopolization or unreasonable restraints of trade, harm competition and the competitive process and therefore constitute unfair methods of competition in violation of Section 5(a) of the FTC Act.”).

78 See Joshua D. Wright & Angela M. Diveley, *Unfair Methods of Competition After the 2015 Commission Statement*, ANTITRUST SOURCE 2-3, 7-8 (Oct. 2015), http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/oct15_wright_10_19f.authcheckdam.pdf (“[O]nly a single form of business conduct—invitations to collude—has been generally accepted as a relatively uncontroversial [Section 5 unfair competition method] violation.”); see, e.g., Fed. Trade Comm’n, *Two Barcode Resellers Settle FTC Charges That Principals Invited Competitors to Collude* (July 21, 2014), <https://www.ftc.gov/news-events/press-releases/2014/07/two-barcode-resellers-settle-ftc-charges-principals-invited>. By contrast, an invitation to collude is not unlawful under the § 1 of the Sherman Act because there is no “agreement” between two parties; a unilateral overture alone is not enough to trigger liability under that statute.

79 15 U.S.C. § 18.

80 See BLOCKCHAIN FOR BUSINESS LAWYERS, *supra* note 27.

concerns are more limited the agencies are less likely to challenge a transaction if there are significant and verifiable transaction-specific efficiencies.⁸¹

Mergers or other transactions that involve rival blockchains may raise antitrust concerns. As part of its analysis, the DOJ or the FTC will consider several factors, including the number and significance of competing blockchains, the likelihood that existing or new firms could and would constrain the combined firm in the future, and efficiencies. Blockchain remains a relatively nascent technology still finding its use cases, with many startups and ventures looking to successfully commercialize the technology. This suggests that competition is dynamic and entry is common. In addition, as described above, blockchains may result in significant cost savings and other efficiencies. This could be a critical part of the analysis, particularly as competition agencies may have relatively less confidence about predicting adverse competitive effects and more confidence in accepting verifiable efficiencies and synergies. The combination or even interoperation⁸² of rival blockchains could potentially result in significant cost savings and other operational synergies that may be credited as part of an agency's merger analysis.

IV. RECENT DEVELOPMENTS IN BLOCKCHAIN AND ASSOCIATED ANTITRUST ISSUES

As a new technology, blockchain has myriad applications. We focus here on a few noteworthy developments based on publicly available materials. The degree of antitrust risk that blockchain participants confront will vary depending on several factors, including blockchain membership composition (does it involve competitors?), industry structure (concentrated, with relatively few firms?), nature of information exchanges (does it involve competitively sensitive information?), information sharing protocols (is access restricted by user? is information encrypted?), and efficiencies (does the venture generate significant cost savings or other synergies?). Recent real world implementations offer useful guidance about how companies navigate these questions when implementing blockchain solutions.

A. IBM Food Trust Supply Chain

The IBM Food Trust—a supply chain solution designed to trace food as it moves from farms to store shelves—is perhaps one of the best known non-cryptocurrency distributed ledger implementations.⁸³ It is a permissioned blockchain built on the Hyperledger open source platform, and participants can enter and control access to their encrypted data by others on the network. A party to a transaction can view only the data that another party has shared. In a matter of seconds, a network user can trace the history of a food item from the time it left the farm to its current location in the supply chain, along with any

81 *Id.*

82 While two different blockchains based on different codebases, architecture, and use cases may be difficult to merge, they can theoretically be made interoperable. *See, e.g.,* Lucas Mearian, *Kadena Launches a Hybrid Platform to Connect Public, Private Blockchains*, COMPUTERWORLD (Jan. 16, 2020), <https://www.computerworld.com/article/3514711/kadena-launches-a-hybrid-platform-to-connect-public-private-blockchains.html>.

83 *About IBM Food Trust*, IBM, <https://www.ibm.com/downloads/cas/EX1MA1OX>.

associated uploaded documents. Data to the network can be uploaded via a web portal or application programming interfaces (APIs) developed by IBM.⁸⁴

Food Trust is designed to increase food safety and freshness, increase supply chain efficiencies, and minimize waste.⁸⁵ Among the participants in Food Trust are some of the biggest competing food manufacturers and retailers, including Albertson's, Unilever, Nestle, Dole Food Company, Tyson Foods, and Kroger.⁸⁶

Food Trust is overseen by an "Advisory Council" composed of industry representatives that set the policies and rules of engagement to maintain the network.⁸⁷

Food Trust illustrates how companies have navigated three critical competition issues that might arise in blockchain collaborations involving competing firms—information sharing, membership composition, and having an objective consensus mechanism.⁸⁸

First, Food Trust illustrates one way to address issues concerning competitively sensitive information. As previously explained, in the United States, information exchanges among competitors are typically analyzed under the rule of reason. In many cases, it will be necessary and reasonable for entities to exchange certain transactional information to accomplish legitimate business goals. However, the amount, type, effect, and nature of the information exchange is crucial to the antitrust analysis. Because the Food Trust participants have complete control over what information they share with the network, they can avoid sharing competitively sensitive information.⁸⁹ To the extent that a participant's competitively sensitive information exists on the network, it is encrypted, preventing competitor access.⁹⁰ Information can be accessed by other participants only if it has been shared on the network, and access has been granted.⁹¹

Second, composition concerns might arise if an interested competitor is refused access. There might be legitimate business justifications to exclude a competitor from a blockchain network, and adhering to a few best practices will minimize antitrust risk. The reasons for membership criteria should be documented, well-defined, and ideally point to procompetitive justifications. Membership criteria also should not be so narrowly defined that they could be construed as purposely excluding a certain competitor or set

84 *Id.*

85 *IBM Food Trust, A New Era for the World's Food Supply*, IBM, <https://www.ibm.com/blockchain/solutions/food-trust>.

86 Ian Allison, *World's Second-Largest Grocer Joins IBM Food Trust Blockchain*, Coindesk (Apr. 11, 2019), <https://www.coindesk.com/worlds-second-largest-grocer-joins-ibm-food-trust-blockchain>.

87 *See About IBM Food Trust*, *supra* note 83, at 11.

88 Beyond Food Trust, there are other sector-wide blockchain networks where similar antitrust risks can arise, especially in the financial technology space. *See Blockchain Gains Traction in FinTech as Payment Networks Emerge*, COMPUTERWORLD (Oct. 28, 2017), <https://www.computerworld.com/article/3234192/blockchain-gains-traction-in-fintech-as-payment-networks-emerge.html>. In addition, there are other blockchain networks within the food supply tracing space. *See Uncover the Human Fingerprints on Your Products*, Fairfood, <https://fairfood.nl/en/solutions/trace>.

89 *See About IBM Food Trust*, *supra* note 83.

90 *Id.*

91 *Id.*

of competitors. When applying the membership criteria, blockchain owners should not treat similarly-situated competitors differently. In addition, reasons for the removal of any member should be well-documented and fall within the established criteria for expulsion preferably detailed at the blockchain's inception or later developed governance structure.

With Food Trust, access is broadly available. Indeed, the only requirement is payment of Food Trust participant access fees.⁹² In addition, the Advisory Council sets the rules of engagement and platform policies, providing members with transparency regarding the decision-making process.⁹³

Finally, a blockchain network can avoid or minimize potential antitrust issues by using a pre-set, objective consensus mechanism, by which no single participant can control how a discrepancy is resolved. This reduces the likelihood that discrepancies raise competitive issues, for instance, based on favoritism or as a result of collusion among competitors on the network. Any deployed consensus mechanism should have discrete and objective parameters explaining how the participants must resolve any discrepancies.

Food Trust incorporates a consensus mechanism by which no party has an outsized influence on how data is on boarded to the network, or how disputes are resolved.⁹⁴ Food Trust uses a “Practical Byzantine Fault Tolerance” trust mechanism, validating addition when a specified number of nodes (usually two out of three, or four out of five) have reached agreement.⁹⁵ And IBM, as the architect of the blockchain has largely left rulemaking to the Advisory Council.⁹⁶

B. Global Shipping Industry

Blockchain technology is being rapidly adopted by the global shipping industry.⁹⁷ The industry is drowning in paperwork required by dozens of governmental agencies, banks, customs bureaus, and other entities.⁹⁸ All of these entities need to sign off on the goods whenever a cargo ship enters or leaves a port, creating a lengthy administrative process dominated by paperwork.⁹⁹

With the adoption of blockchain technology, authorized participants can view the status of goods on the ledger and understand where a container is in transit. In addition, customs documents, bills of goods, and other pertinent paperwork can be accessed in real time. Also, given the anti-tampering architectural properties of blockchain, there is an

92 *IBM Food Trust—Pricing*, IBM, <https://www.ibm.com/products/food-trust/pricing>.

93 *See About IBM Food Trust*, *supra* note 83, at 11.

94 *See id.*

95 *See* Christopher Ferris, *What We Really Mean When We Talk About “Real” Blockchain*, IBM (May 24, 2019), <https://www.ibm.com/blogs/blockchain/2019/05/what-we-really-mean-when-we-talk-about-real-blockchain/>.

96 *See About IBM Food Trust*, *supra* note 83, at 11.

97 Kyunghye Park, *Blockchain Is About to Revolutionize the Shipping Industry*, Bloomberg (Apr. 18, 2018), <https://www.bloomberg.com/news/articles/2018-04-18-drowning-in-a-sea-of-paper-world-s-biggest-ships-seek-a-way-out>.

98 *Id.*

99 *Id.*

inherent assurance that no party has modified, deleted, or appended transactions without consensus from others on the network.

Because these permissioned blockchain networks involve collaborations among carriers, some have sought antitrust exemptions from the Federal Maritime Commission (FMC).¹⁰⁰ The requests for exemption shed light on how to potentially navigate antitrust concerns.

To date, one blockchain shipping network, TradeLens, has received an antitrust exemption, while another request from Global Shipping Business Network (GSBN) is pending before the FMC.¹⁰¹ GSBN is seeking FMC's approval to operate "a blockchain-enabled, global trade digitized process that will enable shippers, authorities and other stakeholders to exchange information on supply chain events and documents."¹⁰² Under the agreement, GSBN will provide participants with: APIs for publishing and subscribing to event data related to cargo; the ability to store and share documents with blockchain participants; and a user interface to view event data and documents, and to manage access permissions.¹⁰³

Given the potentially sensitive nature of information that will be provided on the blockchain network, GSBN proposed measures to address antitrust concerns.¹⁰⁴ The proposed agreement prohibits network participants from sharing with rivals confidential information such as their vessel capacity, customer terms and conditions, or rates and charges that customers will pay.¹⁰⁵ The GSBN petition is based on TradeLens' approved petition, which had sought the same approval in its petition to the FMC.¹⁰⁶

These two agreements offer useful guidance for other blockchain networks. When a network would necessarily involve providing competitively sensitive information, there should be clear parameters of which type of information can and cannot be shared with other blockchain participants at different levels of the supply chain, including prohibitions on sharing with competitor information that could harm competition or facilitate collusion, such as prices. In addition, the governance structure and rules to participate in the blockchain should be transparent and objective to avoid unreasonably disfavoring some blockchain participants or excluding competitors.

100 The U.S. Shipping Act of 1984 prohibits carriers from cooperating on certain matters without FMC's approval. FMC approval is automatic if the Commission fails to reject a proposed agreement within a specified time period. If FMC approves an agreement, federal antitrust laws do not apply to activities carried out in accordance with the agreement.

101 Jeffrey D. Neuburger, *Another Blockchain Supply Chain Shipping Consortium Files for Federal Antitrust Exemption*, NAT'L L. REV. (June 3, 2020), <https://www.natlawreview.com/article/another-blockchain-supply-chain-shipping-consortium-files-federal-antitrust>.

102 *The Global Shipping Business Network Agreement*, Federal Maritime Commission, <https://www2.fmc.gov/FMC.Agreements.Web/Public/AgreementHistory/29502>.

103 *Id.*

104 *See* Neuburger, *supra* note 101.

105 *See id.*

106 Jeffrey D. Neuburger, *Supply Chain Blockchain Initiative Receives Federal Antitrust Exemption*, NAT'L L. REV. (Feb. 11, 2020), <https://www.natlawreview.com/article/supply-chain-blockchain-initiative-receives-federal-antitrust-exemption>.

C. Government Transparency and Antitrust

Antitrust issues also can arise when governments deploy blockchain technology. Specifically, governments are deploying blockchains in an effort to provide greater efficiency, fight corruption, and bring greater transparency to the bidding and procurement process. For example, the U.S. General Services Administration is assessing blockchain to streamline some bids.¹⁰⁷ A pilot program is set to take place in Colombia later this year.¹⁰⁸ While public procurement processes, at least in developed countries, largely occur on electronic systems, blockchains bring something new to the table—they make it more difficult to alter bids or remove records of bids once they have been submitted.¹⁰⁹ Interestingly, the priority placed on greater transparency and increased confidence in the integrity of the records has led Colombia to use a permissionless blockchain instead of a permissioned one.¹¹⁰

In general, while increased transparency can lessen the likelihood of corruption by removing opportunities to tamper with bids, it can also lead to collusive behavior because competitors may have greater access to each other's bids on the open blockchain. The bids might nominally be made pseudonymously, but depending on what information bidders are able to see about rival bidders, competitors might be able to attribute them to particular rivals. This dynamic is even more acute when the number of bidders on a project is small. Such transparency might facilitate anticompetitive agreements because each player can more easily verify that the other is adhering to the agreement by confirming the bid on the ledger. While using blockchain as part of the procurement process is novel, even by blockchain standards, its use could grow, and bid takers should take measures to limit what access competing bidders can access about rival bids and bidders to limit opportunities for collusion.

At the same time, blockchain's procurement application also illustrates another broad point about blockchains being used as evidence in antitrust cases. During investigations and discovery, antitrust agencies and private plaintiffs seek data from the subjects of investigations and litigation, and from other third-party stakeholders. This may include transactional sales data, win/loss data, and pricing data. By their nature, blockchains create a history of information that, unlike other tools, becomes permanent. Bidding records on an open blockchain might be used by antitrust agencies and private plaintiffs to evaluate what information has been exchanged, when the information was exchanged, how competitive behaviors changed post-exchange, and whether there are competitively significant trends in

107 See Stan Higgins, *US Government Seeks Blockchain Solutions for Contract Bidding System*, Coindesk (Jun. 22, 2017), <https://www.coindesk.com/us-government-blockchain-contract-bidding> (“According to a request for quotation published on 19th June, the General Services Administration is looking for a contractor to help it assess how blockchain could be integrated into FASStlane, a system launched last year as part of a broader effort to streamline how smaller companies, especially IT firms, bid on government contracts.”).

108 Rachel Davidson Raycraft & Ashley Lannquist, *How Governments Can Leverage Policy and Blockchain Technology to Stunt Public Corruption*, World Economic Forum (June 15, 2020), <https://www.weforum.org/agenda/2020/06/governments-leverage-blockchain-public-procurement-corruption>.

109 *Id.*

110 *Id.*

the data. Blockchain discovery may also lead to complicated issues of who has ownership or control of the content, including encrypted or access-restricted content.

V. CONCLUSION

Despite falling short of predictions that blockchain would revolutionize the business world (so far), the technology is advancing and being used in an increasing number of applications. Blockchain is finding its use cases, most prominently in fintech, supply chain, insurance, and healthcare contexts, while experimentation continues elsewhere.¹¹¹ Moreover, the technology is evolving and the ways to deploy it are getting easier with the rise of open source platforms and BaaS. As the technology continues to gain traction, participants should pay attention to potential antitrust issues that blockchain presents. Implementations, such as the IBM Food Trust, illustrate how large and sophisticated companies have navigated commercial and competition issues.

To avoid or minimize antitrust risks, participants and administrators of blockchain networks should implement a number of best practices. For example: develop clear governance structures, membership criteria, and an objective consensus mechanism; and establish clear procedural safeguards to the extent the blockchain involves sharing competitively sensitive information between or among rivals. In the end, although blockchain is “old” by technology standards—going on 22 years—this very much remains a new frontier given the relatively limited number of blockchain implementations.¹¹² Private plaintiffs lawyers and governments—legislators and antitrust enforcers—are watching. It is too soon to predict whether blockchain will herald a new era of efficiency across industry sectors or a means to accomplish anticompetitive ends, or both. The next few years will be instructive as existing blockchain efforts mature and new ones launch.

111 Michael del Castillo, *Blockchain 50: Billion Dollar Babies*, FORBES (Apr. 16, 2019), <https://www.forbes.com/sites/michaeldelcastillo/2019/04/16/blockchain-50-billion-dollar-babies/#7feabcd057cc>.

112 Veronica Combs, *William Shatner Explores the World of Blockchain with New Digital Trading Cards*, TECH REPUBLIC (June 25, 2020), <https://www.techrepublic.com/article/shatner-explores-the-world-of-blockchain-with-new-digital-trading-cards>.