MITIGATING ANTITRUST CONCERNS WHEN COMPETITORS SHARE DATA USING BLOCKCHAIN TECHNOLOGY

Almudena Arcelus, Mihran Yenikomshian, Noemi Nocera*

TABLE OF CONTENTS

I. INTRODUCTION: USES OF BLOCKCHAIN TECHNOLOGY FOR DATA MANAGEMENT

Blockchain technology has the potential to reshape many industries, including finance, health care, and any other field that requires data management. While the most popular use case of blockchain technology is cryptocurrency (e.g., Bitcoin), the technology has many more applications and is already redefining the way companies do business.

Fundamentally, blockchain technology is a way to record, process, and authenticate data without centralizing the data or engaging in man-

---

*Almudena Arcelus is a principal at Analysis Group. Ms. Arcelus specializes in the application of economics, finance, and information technology to complex problems in business litigation, and has managed many high-profile litigation projects in technology-intensive industries. Mihran Yenikomshian is a vice president at Analysis Group. Mr. Yenikomshian specializes in data analysis and economic modeling, and he has consulted on economic and strategic issues to companies in a variety of industries, including pharmaceuticals, medical insurance, blockchain and cryptocurrency, computer software and technology, and cybersecurity. Noemi Nocera is an associate at Analysis Group. Dr. Nocera specializes in the application of microeconomics, econometrics, and statistical methods to litigation and government investigations, and has consulted on economic issues in technology and manufacturing industries.

ual processing. Since blockchain technology uses sophisticated encryption methods, it becomes difficult for an individual to manipulate the data. Blockchain technology can be very useful for conducting transactions or collaborating when trust between the parties is low, such as between anonymous people on the internet or between two competitors.

There are two models of blockchain networks: public and private. A public blockchain relies on decentralized governance and is typically open to the public. A private blockchain is operated by an administrator who is responsible for either performing or delegating the task of granting access to the network.

When blockchain technology is used to share data between competitors, legitimate competition concerns may arise regarding the applications. Many collaborations might be driven by economies of scale or scope. However, they could also involve risks associated with new ways of enforcing traditional anticompetitive practices, including active collusion (price-fixing), information exchange, exclusion of competitors, and standard-setting.

Despite the risks, data sharing with blockchain technology might dramatically increase efficiency for an industry, leading to lower costs, or might even be unavoidable, such as if it were to become a requirement of legislation. We argue that most of the antitrust challenges arising from the adoption of blockchain technology can be alleviated when appropriate network design and regulatory oversight strategies are put into place.

II. WHY WOULD COMPETITORS COLLABORATE USING BLOCKCHAIN TECHNOLOGY?

Blockchain technology is a distributed ledger technology whose features makes it amenable to a large variety of applications. The ledger is immutable and tamper-proof thanks to its distributed structure, meaning that it is shared by and synchronized across multiple users, and the use of cryptographic hash functions. Blockchain also allows for the automation of processes that would otherwise need human intervention via the implementation of so-called "smart contracts," computerized transaction protocols (pieces of software) that "automatically execute the terms of a contract."[1] These applications are useful when conducting transactions on the internet when trust between parties is low. Similarly, in the instance of two competitors sharing data, trust may also be

---

1. Jean Bacon, Johan David Michels, Christopher Millard, and Jatinder Singh, *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers*, 25 RICH. J.L. & TECH. 1 (2018), https://jolt.richmond.edu/blockchain-demystified-a-technical-and-legal-introduction-to-distributed-and-centralised-ledgers.

low, and having smart contracts that execute without human intervention when certain conditions are met ensures that no party will gain the upper hand over another by not honoring an agreement.

Because of blockchain's security and automation, potential blockchain applications span numerous industry sectors, including banking, legal services, real estate, stock trading, health data, and food production, among others. The supply chain and autonomous vehicle sectors are two examples of applications that make clear how blockchain solutions can be a source of efficiencies for transacting parties.

A supply chain is a process that provides a path for the movement of goods and services from the supplier to the end customer. Two of the main potential use cases of blockchain technology in supply chain management are product source tracking and automated transactions.[2] In the case of product source tracking, blockchain technology can allow companies and consumers to track the entire product life cycle throughout the supply chain.[3] The technology can provide an indisputable record of all the data related to shipment status, storage environment conditions, and other milestone conditions.

For example, blockchain technology could be used to verify the authenticity of a high-end handbag for sale. The technology would allow a purchaser to see when and where the bag was created and all the entities that took possession of the bag (even temporarily) to the point of sale. This technology could virtually eliminate counterfeiting attempts for many products.

In the case of automated transactions, a blockchain system can act like an incontestable enforcer among all the parties involved in a trade via the use of smart contracts, facilitating financial transactions among unknown parties without dispute. This can ensure safe cargo shipping, even in cross-border trades, and can minimize paperwork, save on labor cost, and ensure data protection. As an example, major software providers such as IBM[4] and Oracle are actively developing private blockchain solutions for firms managing complex supply chains. By thinking of the blockchain as an audit trail to track a particular product throughout its life cycle, firms can gain unmatched insight into the status, condition, and location of every product in the pipeline in real time.

---

2. Jan Keil, *Blockchain in Supply Chain Management: Key Use Cases and Benefits*, INFOPULSE BLOG (Nov. 5, 2019), https://www.infopulse.com/blog/blockchain-in-supply-chain-management-key-use-cases-and-benefits.

3. Shipping and Freight Resource, *How BlockChain Is Improving Supply Chain Management*, WWW.SHIPPINGANDFREIGHTRESOURCE.COM (Oct. 7, 2019), https://shippingandfreightresource.com/how-blockchain-is-improving-supply-chain-management.

4. *See* Sanjeev Verma, *How Blockchain and IoT is Making Supply Chain Smarter*, BLOCKCHAIN PULSE: IBM BLOCKCHAIN BLOG (Nov. 19, 2019), https://www.ibm.com/blogs/blockchain/2019/11/how-blockchain-and-iot-is-making-supply-chain-smarter.

A second application of blockchain is related to the automotive industry in general and to autonomous vehicles (AVs) in particular. Autonomous vehicles, or self-driving cars, are vehicles capable of sensing the environment and moving safely with little to no human input. The AV technology, when widely implemented, has a potential for disruption in multiple areas, including shipping, human transportation, and vehicle ownership.

There are various fundamental applications of blockchain to the development of AV technologies, but the most promising application relates to sharing test data and digital identities. Developing autonomous technologies requires testing, which can be expensive and time consuming, and, especially when it comes to actual road testing, requires multiple permits and authorizations. This can dramatically limit the amount of data that each company can obtain and process.

In addition, most vehicle manufacturers operate in fierce competition with each other and have little incentive to collaborate on research or exchange data freely. Blockchain technology can deliver a solution in which each piece of data is catalogued, labeled, and immutably branded by the company that generated it. All the data can then be traded[5] between different companies in an open market, which can facilitate cooperation between competitors and significantly speed up the development of AV technologies.

Such solutions can be applied to many different fields of research, accelerating the development in multiple areas of technology. For instance, the Mobility Open Blockchain Initiative (MOBI), a project currently testing these ideas, includes prominent members from the automotive industry that normally compete with one another, such as BMW, Ford, GM, Honda, and Renault.[6] Another project in this sector is Toyota's partnership with the Massachusetts Institute of Technology (MIT)[7] to explore a blockchain solution to the management of vehicle testing data. Finally, IOTA, a permissionless distributed ledger technology firm, has announced several recent partnerships in this sector. These include a 2018 partnership with Volkswagen[8] to develop a Digital Car Pass to collect and communicate car data, and a partnership

---

5. *See* Blockchain Central, *IoT Automotive: Digital Identity for Autonomous Vehicles*, BLOCKCHAIN CENTRAL (Aug. 5, 2019), https://www.youtube.com/watch?v=YUm0lGzN7QY.

6. MOBI, MOBILITY OPEN BLOCKCHAIN INITIATIVE, https://dlt.mobi (last visited, Feb. 3, 2021).

7. Toyota – CSAIL, https://toyota.csail.mit.edu (last visited, Feb. 3, 2021).

8. Chris Mueller, *Volkswagen and IOTA Build the Future*, IOTA NEWS (May 27, 2019), https://iota-news.com/volkswagen-and-iota-build-the-future.

with Jaguar Land Rover[9] to develop a smart wallet for vehicles, ena-bling drivers to earn money and pay for selected services while on the go.

III. WHAT ARE THE CONCERNS ABOUT ANTICOMPETITIVE USES OF BLOCKCHAIN?

Despite the potential efficiency gains spurred by collaboration on blockchain platforms, some have argued that the adoption of block-chain technology by firms will lead to anticompetitive outcomes.

Networks with distributed ledgers that make certain sensitive data, such as price, accessible to competitors potentially could aid in collu-sion, such as price-fixing and bid-rigging. Specifically, competitors that form or participate in blockchain ventures might use price, cost, or out-put data to enter into unlawful horizontal agreements.[10] Because the ledger is distributed, everyone has access to everyone else's transaction data, which contain prices and quantities. This could provide cartelists with a very powerful monitoring tool to detect deviation from agreed-upon prices, as well as transparent data that allow those who collude to reach terms on price or market share, for example. Firms in oligopolis-tic markets may achieve cooperation tacitly with this level of infor-mation.

Additionally, some believe[11] that if a specific private, permis-sioned blockchain network becomes critical to competing in a market, it is possible that certain competitors could be excluded from the block-chain and thereby be barred from competing in the market, depending on who administers the network. This could occur if relevant players in a particular market coexist in the same permissioned blockchain and hold the credentials to grant access. In such a scenario, these players may have an incentive to prevent new firms from entering the block-chain. Entrants would then need to compete without this resource.

Finally, if a market relies on a decentralized network, governments may not have entry points into the network to enforce regulations, and might also have trouble identifying perpetrators if the network offers users anonymity.[12] Identification issues are particularly acute for pub-lic, anonymous blockchains, such as the one implemented for Bitcoin, while entry points may be contentious in permissioned blockchains.

---

9. IOTA Foundation, *Earn as You Drive With Jaguar Land Rover and IOTA*, IOTA BLOG (Apr. 29, 2019), https://blog.iota.org/earn-as-you-drive-with-jaguar-land-rover-and-iota-3c744d8c0cba.

10. *See* Thibault Shrepel, *Collusion by Blockchain and Smart Contracts*, 33 HARV. J.L. & TECH. 1 (2019), https://jolt.law.harvard.edu/assets/articlePDFs/v33/03-Schrepel.pdf.

11. *See* OECD, *Blockchain Technology and Competition Policy*, Issues paper by the Sec-retariat (2018), https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf.

12. Thibault Shrepel, *Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox*, 3 GEO. L. TECH. REV. 281 (2019).

Consequently, we believe that the impact blockchain has on competition will depend on whether firms actively utilize thoughtful network design strategies to promote competition, and whether regulators create and enforce clear guidelines for firms to follow while designing and operating their blockchain networks. We discuss these points in the next section.

IV. WHAT ARE POTENTIAL WAYS TO MITIGATE ANTICOMPETITIVE CONCERNS?

Regulators and firms are actively considering how to offset the antitrust risks associated with blockchain adoption. Firms must first identify what type of blockchain network best suits their business needs, and then they should employ strategic design tactics to offset potential antitrust risks associated with the chosen network type. In this section, we discuss three sets of network design strategies that can help alleviate competition issues arising from the adoption of the technology: 1) sensitive data management; 2) centralized governance; and 3) transparency for regulators.

A. Sensitive data management

Three steps can be taken to mitigate the risk when competitors share sensitive data via distributed ledgers. First, certain particularly sensitive data on the blockchain could be encrypted and made visible only to select users who have received a special key, thereby limiting which transaction details those without the key can see. Second, network administrators can use firewalls to manage which users have access to data stored on the network. Last, forward-thinking network designers could decide to keep certain more sensitive data off the blockchain and instead store such data on privately managed non-blockchain servers.

Network designers should carefully consider the types of data that should be encrypted and included in the blockchain, data that should be unencrypted and included in the blockchain, and data that should be excluded from the blockchain altogether. As a safeguard, designers should only include data that are mission critical and exclude data that do not have a specific and important business requirement.

B. Centralized governance

At least three types of centralized governance strategies can offset the risk of competitor exclusion and inhibited regulation. First, regulators can offer guidance on how to define clear membership rules for

accessing networks, and through oversight be sure that firms direct administrators of their centralized blockchains to incorporate and enforce those rules. Second, centralized blockchain administrators can design entry points that give regulators their own special access to networks so that they can carry out enforcement measures. Last, administrators of centralized networks can iteratively encode measures directly into the governance to define appropriate actions on the network and combat anticompetitive behavior both before and after it occurs.

C. Transparency for regulators

Implementing transparency in the network design can improve regulators' ability to investigate claims of antitrust violations. First, blockchain networks could be designed to provide antitrust investigators with a clear audit trail of the life cycle of an asset as it moves through a firm's supply chain, providing critical information to investigators as they assess when and how a firm's products transformed from raw materials to a finished good. Second, networks can be designed to provide investigators with more accurate, reliable, and comprehensive transaction data across an entire firm, rather than the piecemeal and inconsistent data that regulators often receive. Last, we could imagine the development of a blockchain, potentially accessible only by select parties or regulators, that contains industry-wide transaction data, which could provide an unmatched tool for investigators. Furthermore, the standardized data format in a blockchain may lead to faster resolution of potential antitrust investigations.

Whether or not these particular strategies would be effective in a real-world setting will depend on the industry or business context, the design of the blockchain network at issue, and the effectiveness of governance and regulatory oversight.

V. Conclusion

Because of its potential to change the way many governments' and firms' services currently operate, blockchain technology has attracted extensive press coverage. Although antitrust concerns exist in relation to blockchain adoption and data sharing between competitors (including access to information, collusion, abuse of dominance, and enforcement), blockchain serves mainly as a data management tool. How it affects competition will depend on network design and regulatory oversight, among other things. When examining antitrust concerns, industry observers as well as regulators should assess blockchain technology according to its specific implementation and its role in the wider framework within which it is used.