JONES DAY | One Firm Worldwide℠

WHITE PAPER

August 2018

Blockchains and Antitrust: New Technology, Same Old Risks?

Blockchain technology can allow for more efficient and more secure business transactions across a number of industry sectors. Still, anticompetitive practices carried out by blockchain participants remain subject to antitrust scrutiny in the jurisdictions in which they operate, including in the United States, Europe, and Asia, where regulators are paying increasing attention to the potential for collusive or exclusionary conduct.

This Jones Day *White Paper* describes how blockchain participants can manage risk by implementing precautions and safeguards designed for the specific features of blockchain technology.

TABLE OF CONTENTS

"Pay no attention to that man behind the curtain."—The Wizard of Oz

Blockchain or "distributed ledger" technology links parties to a transaction together behind a curtain of technology that defines membership and information access rights. This virtual curtain offers the potential for more efficient and secure transactions without the need for a centralized authority. The most popular real-world example of this technology is the cryptocurrency Bitcoin. Unlike a traditional financial system, in which a bank is the essential intermediary, Bitcoin operates without a centralized authority; instead, users exchange bitcoins directly.

Over the years, blockchain and derivative technologies have extended beyond cryptocurrency into supply-chain activities and other sectors, including health care, property rights, and insurance, where it is critical to track and record information about pricing, units, or other key specifications.

Many blockchain initiatives involve collaborations among competing firms in public ("permissionless") or private ("permissioned") ledgers. Most blockchains for business applications involve private ledgers. These private ledgers operate out of public view.

Yet any anticompetitive practices that stem from these private blockchains still are subject to antitrust scrutiny. A blockchain, like any other situation in which marketplace rivals share information, may raise the potential for unlawful coordination or exclusionary conduct that violates the antitrust laws in the United States and around the world. To the extent that a blockchain operates across borders, it likely is subject to the competition laws of multiple jurisdictions. Competition authorities are paying close attention to the technology as it gains prominence.

For example, in February 2018, the European Commission announced the "EU Blockchain Observatory and Forum."[1] In March 2018, the U.S. Federal Trade Commission announced the creation of an internal "FTC Blockchain Working Group."[2] In April 2018, the OECD published an issues paper titled, "Blockchain Technology and Competition Policy."[3]

This *White Paper* highlights potential U.S. antitrust issues that may arise in the formation and operation of blockchains, especially private platforms, and discusses measures that companies can take to minimize antitrust risk.

BLOCKCHAIN BASICS

A blockchain is a decentralized, electronic register in which transactions can be recorded in a verifiable and permanent way. Records of transactions are stored along with other transactions into "blocks" of data that are linked to one another in a "chain." The register or database is hosted by a number of different users or "nodes." Blockchain users are assigned unique identifiers—for Bitcoin, these are public and private encryption keys—that identify each participant to a transaction. Each block is recorded using an algorithm that encoded every prior block in the blockchain. Thus, once a block is added to the chain, it is virtually impossible to modify. Any change would require modifying every subsequent block of data on the chain. And because each participant on the blockchain has a unique identification key, other users can instantly verify prior transactions involving that participant.

There are two types of blockchains: public ledgers are open and permissionless, and private ledgers are closed and permissioned.

Public Blockchains

A public blockchain is open to all, but its participants can remain pseudonymous behind unique user identifiers within the network. The ledger tracks each participant by its identifier. The ledger is transaction-based, and it notes the prior transaction history. This information can be used to assess if the participant has sufficient funds, capacity, inventory, etc. to complete the requested transaction based on the prior transactions that either have credited or debited the account. Without a central authority or clearing house, each node is responsible for keeping a ledger of all participants' transactions.

Anyone can propose blocks of transactions to be added to public blockchains. There is no central validation system that oversees the blockchain to determine which blocks of transactions get added or to determine which are valid when discrepancies occur. Instead, blockchains use preset rules, a "consensus mechanism," to decide which record should prevail.

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. This is called "mining." The nodes on the network signal their acceptance of the proposed

block by adding it to their copies of the 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. If there is a conflict between different versions of the blockchain, the chain that has the largest amount of computational work is considered to have the accurate record under a "proof of work" protocol. Under this system, there is no practical likelihood that one participant can be strategically prioritized or given an unfair advantage over another. To the extent disputes arise between participants, there are no default rules on how to resolve them.

Public blockchains are well suited for transactions in which participants need pseudonymity and the ability to transact with an unlimited number of other participants. However, some public blockchains have technical barriers, such as speed, scalability, and storage constraints. These limitations present impediments for business applications in which multiple transactions need to occur quickly and efficiently. Indeed, it takes approximately 10 minutes to process one block of Bitcoin transactions. Other public blockchains, such as the Ethereum blockchain network, have improved on some of these limitations, for example, by processing transactions faster. Confronted with these challenges, private blockchains have been developed to maintain efficiency and to address some of the fundamental technological constraints of public blockchains.

Private Blockchains

Private blockchains are hosted by a defined set of nodes in which only permitted users have read and write access. In these collaborations, there are likely to be fewer participants, greater potential for information-sharing among participants, and less visibility into transactions from outside the blockchain. In this respect, private networks lose many of the hallmarks of the original form of the technology, which makes possible pseudonymous transactions in an open system.

Unlike public blockchains, private distributed ledgers:

- 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 owners or designated participants that are responsible for resolving discrepancies, often outside of a proof-of-work system;
- Have a limited membership, often without user anonymity; and
- Host data that is not readable or writable to the public, so the information exchanged cannot be reviewed by non-members who lack access.

These attributes make private ledgers attractive for many business applications. Private blockchains can scale significantly better than public blockchains because they 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.

ANTITRUST ISSUES

Blockchain and other "high tech" initiatives, such as artificial intelligence and "big data," are evaluated under the same antitrust laws and analytical framework as "old tech" conduct. In the United States, use of blockchain technology raises potential issues under Sherman Act § 1 (no collusion), Sherman Act § 2 (no monopolization), Federal Trade Commission Act § 5 (no unfair competition), and Clayton Act § 7 (no anticompetitive mergers).

No U.S. antitrust enforcement actions have been brought involving blockchains to date. However, in 2015, the Department of Justice ("DOJ") brought charges against an e-commerce retailer and two executives for price-fixing, alleging that the conspirators used a pricing algorithm to create an artificial pricing floor for posters and other decoration (*Wall Décor*).[4] The conspirators agreed to use pricing software to lower prices only as far as the lowest price established by a non-conspiring competitor. The conspirators thereby effectively eliminated their competition that could have resulted in lower prices for consumers.

Similar to the defendants in the *Wall Décor* case, who used a pricing algorithm to reduce competition, private blockchain participants could use their transaction data to set and monitor prices or to prevent prices from dropping to "unfavorable" levels.

Collusion—Sherman Act § 1

In recent years, competition regulators and mainstream media in the United States and around the world have devoted

significant attention to the question of whether technology companies (e.g., Facebook, Apple, Amazon) and "high tech" products or services should be subject to different antitrust enforcement rules. But as a Department of Justice Antitrust Division official recently explained:

> 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.[5]

This statement implicates Sherman Act § 1, which prohibits anticompetitive collusion, such as price fixing, bid rigging, or market allocation.[6] Depending on how a blockchain is formed and operated, it also could implicate antitrust laws that prohibit monopolization and anticompetitive transactions. For most blockchain collaborations among rival businesses, however, the greatest practical antitrust risk involves collusion. 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.

A Section 1 violation requires concerted action (an "agreement") between two or more firms. The formation of a blockchain, without more, cannot result in antitrust liability. 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 organized validation of 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. Similar to the defendants in *Wall Décor*, rivals could use private blockchains to facilitate a naked price-fixing arrangement that constitutes a *per se* violation of Section 1 without regard to actual or claimed procompetitive effects.

Absent a price-fixing agreement, blockchain members could still violate Section 1 if they use the technology 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 not *per se* unlawful. 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.

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

- Source of the information provided (actual or potential competitors);
- Nature of the information exchanged (competitively sensitive);
- Industry structure (number of competitors); and
- Whether the legitimate business goals could have been achieved with less or no exchange of competitively sensitive information (less-restrictive alternative).

In addition, private blockchain participants also may face Section 1 risk if they exclude competitors from the blockchain. If a blockchain were to become critical to compete in a particular industry, competitors may need to be a part of the blockchain. For example, there are certain industries in which scale and scope are important. In banking, using blockchain technology can significantly reduce transactions costs. In health care, providers may not be able to provide the same level of care or to generate necessary operating efficiencies without access to blockchain data networks, pharmaceutical supply chains, or resource management.

If private blockchain members exclude competitors from accessing a blockchain that has become essential to doing

business, nonmembers may not be able effectively to compete. Excluding rivals from a blockchain considered to be a "must have" in the industry may give rise to claims that the blockchain's membership rules are being used to limit competition.

Exclusionary conduct also can occur from within the blockchain. In private blockchains, owners or designated blockchain participants have the authority to resolve discrepancies in the chain. These discrepancies may not be resolved under an objective consensus mechanism. Rather, owners and/or designated participants may have the power unilaterally to resolve discrepancies. Certain participants could agree to resolve discrepancies against rival competitors and to prioritize others.[7] Although an agreement to exclude a competitor is analyzed under the rule of reason, excluding a rival solely to impede its ability to compete is not a legitimate business justification that can offset evidence of anticompetitive conduct.

Monopolization—Sherman Act § 2

Sherman Act § 2 prohibits monopolization and attempts to monopolize.[8] But monopoly power alone is not enough for a Section 2 claim. Rather, the entity must use its monopoly power to willfully maintain that power through anticompetitive exclusionary conduct. Courts have found exclusionary conduct in a number of circumstances, including 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.

Blockchains may lead to a Section 2 violation if, for example, a supplier 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 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 refused to sell a product to a competitor that it made available to others, or when a monopolist had a prior course of dealing with the competitor but then terminated the relationship without any legitimate business reason. 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.

Unfair Competition—Federal Trade Commission Act § 5

Section 5 of the FTC Act prohibits unfair competition.[9] 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" that causes harm to competition, including conduct that is not covered by the Sherman Act.[10] One area in which the FTC has recently exercised its Section 5 authority is to challenge invitations to collude—efforts by one firm to one or more of its competitors to enter an anticompetitive price-fixing or market-allocation agreement. By contrast, such an invitation to collude is not unlawful under Section 1 of the Sherman Act as there is no "agreement" between two parties.

Blockchains facilitate information exchanges among all participants. As discussed above, the exchange of competitively sensitive information in real-time transactions may lead to price fixing or bid rigging among competitors. However, blockchains need not be limited to current transactions. Blockchains also may post future prices or bid information. Under certain circumstances, posting this prospective information, known as "signaling," may be viewed as an invitation to collude in violation of Section 5, particularly if there is evidence that subsequent transactions and posted prices were impacted by the signal.

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.[11] The key question is whether the proposed transaction is likely to create or enhance market power or to facilitate its exercise. A transaction is less likely to be anticompetitive if entry or repositioning is easy or if the merged firm and its remaining rivals could not profitably raise prices or reduce competition. In addition, the agencies are less likely to challenge a transaction when there are significant transaction-specific efficiencies.

Mergers or other transactions that involve rival blockchains may raise antitrust concerns. As part of its analysis, the DOJ and FTC 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 is still a relatively nascent

technology. There are more than 1,000 blockchain startups and hundreds of new and expanding corporate blockchain ventures.[12] This suggests that, in general, competition is dynamic and entry is relatively common. In addition, as described above, blockchains may result in significant efficiencies. The combination 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.

ANTITRUST RISK AVOIDANCE

The vast majority of blockchain ventures are likely procompetitive or competitively neutral. The degree of antitrust risk that confronts blockchain participants will vary depending on several factors, including composition (does it involve competitors?), industry structure (is it 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?). Blockchain participants can take steps to minimize their antitrust risk.

Narrowly Tailor the Exchange of Competitively Sensitive Information

Information exchanges among competitors are analyzed under the rule of reason. In many cases, it will be reasonable, and perhaps even necessary, for entities to exchange certain transactional information to accomplish legitimate business goals. However, the amount, type, and nature of the information exchange is crucial to the antitrust analysis. If possible, competitors that participate in a blockchain should avoid sharing competitively sensitive information, especially in concentrated industries. If competitively sensitive information must be shared, consider encrypting the sensitive data so that rivals cannot access the data. For example, encryption is critically important in the health care space. Only those entities in the blockchain that are the intended recipients of the data should have the ability to access and read the block of information.[13]

In addition, parties should consider which employees have access to the information within their organizations and how the information is used. Competitively sensitive information within the blockchain should be firewalled from employees who have responsibility over pricing, marketing, strategy, and other competitively important decisions. Doing so minimizes the risk that this information will be used to reduce competition between participants.

Use Well-Defined, Inclusive, and Justifiable Criteria for Membership

Reducing the computational expense of consensus mechanisms by forming a private blockchain of trusted members can provide greater scalability and efficiencies. The composition of the blockchain—number, size, and competitive significance of its members—can directly impact operational efficiencies. Therefore, membership criteria can be an important element of a successful blockchain.

Antitrust issues most often arise in this context when an interested competitor is refused access. Although there may be legitimate business justifications to exclude a rival, adhering to several best practices will minimize antitrust risk. The reasons for membership criteria should be well-documented and well-defined, and they should point to procompetitive justifications. Criteria should also not be so narrowly defined that it could be construed as purposely excluding a certain competitor or set of competitors. When applying the membership criteria, owners of the blockchain should not treat similarly situated competitors differently. Reasons for expulsion should be defined and known to all members. Finally, reasons for the removal of any member should be well-documented and fall within the established criteria for expulsion outlined at the formation of the blockchain.

The size of the blockchain also may impact antitrust risk. The fewer the number of participants in the blockchain, the easier it may be to source competitively sensitive information to a specific participant. Blockchain administrators may try to use anonymity to obscure competitively sensitive information and to minimize the likelihood of collusion and unlawful information exchanges.

In private blockchains, however, more restrictive membership criteria necessarily shrinks the pool of eligible firms. If member competitor X is an outlier in terms of price, capacity, inventory, or other characteristics, and that information is exchanged in the blockchain, rival members may be able to determine that competitor X is a party to the transaction. This albeit indirect transparency may increase antitrust risk. By increasing the number of competitors and by diversifying the membership pool,

anonymity becomes more effective at concealing transaction participants and their data, which decreases antitrust risk.

Use an Objective Consensus Mechanism

As discussed above, an owner, operator, or its designee that serves as the membership "gatekeeper" may have the ability to control how data disputes are resolved. It also may restrict which participants have the right to read/write/fix discrepancies. These procedural rules could potentially allow exclusionary practices to occur from within the blockchain. The owner, along with the designated participants, may agree to disadvantage certain competitors.

By resolving discrepancies using a pre-set, objective consensus mechanism, such as proof of work, no single participant can control how a discrepancy is resolved. This reduces the likelihood that discrepancies will raise competitive issues, for example, based on favoritism or as a result of collusion among rival members. If a different system must be deployed, discrete parameters should be established explaining how the designated participants must resolve the discrepancy. Such a system could include, for example, having discrepancies or disputes resolved by a rotating, random set of participants.

Consider How Blockchain Data Will Be Used as Evidence

Antitrust agencies often seek data from the subjects of investigations and from other third-party stakeholders. This may include transactional sales data, win/loss data, and pricing data. By their nature, blockchains create a long history of information that, unlike other tools, becomes permanent as discrepancies are resolved by those participating in the blockchain. Antitrust agencies can use this data 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 the data.

CONCLUSION

Before the internet, cell phones, email, and other modern-day communication technologies, unlawful price-fixing agreements and improper information exchanges were usually carried out in person, behind closed doors, in smoke-filled rooms. Over time, business communications and related technologies have evolved. Communication options exploded (emails, texts, tweets, etc.). Conversations could be "deleted," "erased," or "shredded."

With the formation of blockchains, particularly private blockchains, there is a technological curtain behind which business transactions can occur, forming a potentially permanent record of information. Alongside the extraordinary utility and potential efficiencies of blockchain technology, there is potential antitrust risk. To manage that risk, participants should evaluate the need to implement precautions and safeguards that are tailored to account for the specific attributes of blockchain technology.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Ryan C. Thomas
Washington
+1.202.879.3807
rcthomas@jonesday.com

Mark W. Rasmussen
Dallas
+1.214.220.3939
mrasmussen@jonesday.com

Stephen J. Obie
New York / Washington
+1.212.326.3773 / +1.202.879.5442
sobie@jonesday.com

Harriet Territt
London
+44.20.7039.5709
hterritt@jonesday.com

Craig A. Waldman
San Francisco / Silicon Valley
+1.415.875.5765 / +1.650.739.3939
cwaldman@jonesday.com

Larissa C. Bergin
Washington
+1.202.879.5499
lbergin@jonesday.com

ENDNOTES

1 "European Commission launches the EU Blockchain Observatory and Forum," European Comm'n (Feb. 1, 2018).

2 "It's Time for a FTC Blockchain Working Group," Fed. Trade Comm'n (Mar. 16, 2018).

3 "Blockchain Technology and Competition Policy," Organisation for Economic Co-operation and Development (Apr. 26, 2018).

4 *See, e.g.*, Press Release, U.S. Dep't of Justice, "E-Commerce Exec and Online Retailer Charged with Price Fixing Wall Posters" (Dec. 4, 2015); *see also* Plea Agreement, *United States v. Topkins*, No. 15-cr-00201 (N.D. Cal. Mar. 30, 2015).

5 Andrew Finch, Principal Deputy Ass't Att'y Gen., Antitrust Div., U.S. Dep't of Justice, Remarks at New York Antitrust in the Financial Sector: Hot Issues & Global Perspectives (May 2, 2018).

6 15 U.S.C. § 1.

7 "[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." Colin Thompson, "Private Blockchain or Database? How to Determine the Difference," *The Blockchain Review* (Oct. 4, 2016).

8 15 U.S.C. § 2.

9 15 U.S.C. § 45.

10 *See, e.g.*, Complaint at 31, *FTC v. Qualcomm Inc.*, 2017 WL 242848 (N.D. Cal. 2017) (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.").

11 15 U.S.C. § 18.

12 "Outlier Ventures," *Startup Tracker* (listing 1,349 blockchain start-ups as of March 29, 2018); "Outlier Ventures," Corporate Research Tracker (listing 293 corporate blockchain ventures as of March 29, 2018).

13 *See* Elizabeth Snell, "Data Security Key Considerations for Healthcare Blockchain Success," *Healthcare Security* (Mar. 26, 2018).