

## ANTITRUST TRADE &amp; PRACTICE

# Antitrust Considerations for Private Permissioned Blockchains

By Karen Hoffman Lent and Kenneth Schwartz

April 4, 2025

In the first few months of his presidency, President Donald Trump has already taken significant steps toward fulfilling his campaign promise to limit the regulation of digital assets and to promote the adoption of blockchain technology.

This regulatory posture, which stands in sharp contrast to the approach of the Biden administration, is likely to spur increased use cases of blockchain technology. In this article, we outline some of the antitrust concerns that could arise if groups of competitors develop and implement private, permissioned blockchains.

## Blockchain Basics

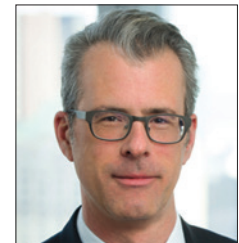
Blockchains are a type of technology that, through cryptography, allows data to be shared across a decentralized network and creates a ledger of verified and immutable transactions shared among network participants.

In order for users to trust such a decentralized structure, both the underlying computer code and each transaction are transparent. In effect, a blockchain can be seen as a decentralized digital ledger with secure and immutable transaction information viewable by all network participants.

While blockchains are often associated with cryptocurrencies, they have potential uses in any



By **Karen Hoffman Lent**



And **Kenneth Schwartz**

situation where parties are transacting in information and want to do so in a decentralized but secure manner. This might include supply chain management, financial transactions, and general record-keeping.

Today, the majority of blockchains are so-called permissionless, “public” chains that are freely available for anyone to access and use, and for which anyone can act as a validator of the transactions flowing through the network.

However, the transparency of public blockchains can create issues for entities who do not want their transactions to be viewable by the general public, or who are concerned about sharing a network with unknown participants. These entities might therefore create or participate in private, permissioned blockchains.

Such blockchains share many of the attributes of public blockchains, but are only accessible to a limited set of participants, each of whom

needs to be approved to join the network. Only the private blockchain participants can view on-chain transactions.

### **Procompetitive Effects of Utilizing Blockchain**

Blockchain technology can generate substantial efficiencies and procompetitive effects, including reduced transaction costs, increased database accuracy and reliability, and enhanced operational transparency and security.

For example, supply chain management is a key application because a blockchain can provide an immutable record, tracking products from production to delivery. This reduces fraud, improves traceability, and ensures product authenticity,

While blockchains are often associated with cryptocurrencies, they have potential uses in any situation where parties are transacting in information and want to do so in a decentralized but secure manner

especially in industries like pharmaceuticals, food, and luxury goods.

Additionally, businesses can use blockchain technology to ensure secure data and record management. In particular, where companies are responsible for storing and sharing extensive customer records, such as in healthcare, insurance, real estate, and financial services, a blockchain can enhance the accurate and secure transfer of customer information.

For example, medical care providers often complain that they cannot provide the best care because patient records are scattered across different systems, leading to delays in patient care, security risks, and inefficiencies while they locate patient records.

However, a private blockchain network accessible to authorized healthcare providers could resolve these issues. When a patient visits an authorized healthcare provider, the provider could access the blockchain that includes the patient's records and add new records, which are then permanently accessible to other authorized healthcare providers.

### **The Current Regulatory Climate**

Substantively, Trump sought to create an unambiguous regulatory framework that would spur the growth of technologies like blockchain.

In an Executive Order titled *Strengthening American Leadership in Digital Financial Technology*, issued during his first week in office, Trump declared that it was his administration's policy "to support the responsible growth and use of [ ] blockchain technology, and related technologies across all sectors of the economy, including by: (i) protecting and promoting the ability of individual citizens and private-sector entities alike to access and use for lawful purposes open public blockchain networks without persecution." Exec. Order No. 14178, 90 Fed. Reg. 8647 (Jan. 23, 2025).

Additionally, the Secretary of Commerce, Howard Lutnick, recently stated that "[t]echnology is at the foundation of the Trump presidency . . . The blockchain [is] a key part of that thinking and embracing that." Howard Lutnick, Secretary, Dep't of Commerce, Remarks by President Trump at the White House Digital Assets Summit (Mar. 7, 2025).

This policy represents a minor shift from the first Trump Administration. During President Trump's first term, the then-chief antitrust enforcer at the Department of Justice (DOJ), Makan Delrahim, acknowledged blockchain's "revolutionary potential" while also acknowledging potential antitrust risks associated with the use of blockchain technology, stating that "many astute observers of blockchain technology have raised questions about its implications for collusive activity.

Blockchain solutions might . . . facilitate sharing of competitively sensitive information" and "[i]ncumbents could use blockchains anticompetitively to exclude competition." Makan Delrahim, Former Assistant Attorney General, Remarks at the Thirteenth Annual Conference on Innovation Economics (Aug. 27, 2020).

Nevertheless, Trump has also appointed a White House A.I. & Crypto Czar, and nominated chairs to the Securities Exchange Commission (SEC) and the Commodity Futures Trading Commission, all of whom are generally perceived as crypto-friendly.

Further, the SEC under the current administration has dismissed a number of high-profile lawsuits and closed ongoing investigations in the cryptocurrency and blockchain space. Collectively, these moves signal a broad shift in enforcement strategy with a hands-off regulatory approach.

### **Potential Antitrust Issues with the Use of Blockchain**

Although the Trump Administration has signaled its embrace of blockchain technology, and appears unlikely to prioritize enforcement actions against blockchain-based use cases, companies participating in private blockchains must remain cognizant of antitrust law.

While the Trump Administration's actions in this space have not implicated the Federal Trade Commission (FTC) or the Antitrust Division of the United States Department of Justice (DOJ)—the federal agencies tasked with enforcing the antitrust laws—a lack of antitrust enforcement to date does not mean that blockchain-related conduct will avoid scrutiny.

Even in the absence of government action, private plaintiffs remain free to enforce the federal and state antitrust laws. See 15 U.S.C. §15(a).

Private blockchains could theoretically be used by competitors to facilitate conspiracies, information exchanges, and group boycotts that potentially violate the antitrust laws.

Despite the lack of antitrust suits to date challenging the use of a blockchain network, companies should not interpret Trump's pro-blockchain comments as conferring immunity for competitor conduct engaged in through a private blockchain that would otherwise violate the antitrust laws if it occurred outside of the context of a private blockchain network.

The antitrust laws, and their public and private enforcement, remain in full effect.

For example, private, permissioned blockchains could potentially serve as covert means for competitors to share competitively sensitive information (including prices, output, bids, and customer-specific features and specifications), coordinate with one another, and track each other's compliance with the cartel's terms without alerting non-cartel members of their unlawful conduct.

In essence, a private blockchain network could hypothetically eliminate the need for competitors to gather to discuss the terms of an unlawful conspiracy because they could simply input competitively-sensitive information on the blockchain.

Because this conduct would likely constitute unlawful collusion if it occurred over text, through phone calls, or during an in-person conversation, it would likely also be unlawful if it occurs using a blockchain.

By way of analogy, courts have denounced the sharing of competitively sensitive information where the information exchanged was not publicly disseminated, which is also true of information on a private blockchain. See, e.g., *Sugar Inst., Inc. v. U.S.*, 297 U.S. 553, 604-05 (1936); *Am. Column & Lumber Co. v. United States*, 257 U.S. 377, 409 (1921); *Todd v. Exxon Corp.*, 275 F.3d 191, 213 (2d Cir. 2001) (Sotomayor, J.) (noting that private information exchanges, without public dissemination of the information, lose most of their "procompetitive potential").

During the Biden Administration, the DOJ took the position that "information sharing alone can violate Section 1, even without proof of an agreement to fix prices." Statement of Interest of the United States, *In re Pork Antitrust Litig.*, 665 F. Supp. 3d 967 (D. Minn. 2024).

However, the DOJ's Statement of Interest in *In re Pork Antitrust Litigation* does not provide guidance concerning key issues relevant to information exchanges, such as whether there needs to be proof of a mutual agreement or whether the individuals responsible for the information exchange must have pricing authority in order for an information exchange to violate Section 1.

The DOJ's Statement of Interest also did not acknowledge any of the potential procompetitive justifications of information exchanges—including increased efficiency and innovation, and more accurate pricing and production—that could overcome a Section 1 claim under the rule of reason.

Antitrust scrutiny of other technologies, including online chatrooms and pricing algorithms, demonstrates how regulators and private plaintiffs might evaluate information exchanges on a blockchain network.

Just like a private blockchain network is shielded from the eyes of government regulators and third parties, an online chatroom is similarly opaque and difficult to monitor. Plaintiffs have increasingly alleged that competitors utilized online chatrooms to facilitate their alleged conspiracies.

Likewise, the use of pricing algorithms, which can be used to set prices by analyzing data, and which may provide pricing recommendations or automatically adjust prices, also occurs in private.

And, like blockchain networks, pricing algorithms can be procompetitive by facilitating more competitive, informed pricing decisions that accurately reflect market demand. The recent skepticism of algorithmic pricing provides

---

Private blockchains could theoretically be used by competitors to facilitate conspiracies, information exchanges, and group boycotts that potentially violate the antitrust laws.

important context for how antitrust law could be used to challenge allegedly collusive behavior by entities using a private blockchain.

Furthermore, private blockchain participants could potentially face allegations of Section 1 violations—especially from entities that were denied permission to the private network—for a group boycott if they exclude competitors from accessing a blockchain.

This is particularly likely if larger companies in a given industry were to use their control over a private blockchain network to exclude smaller competitors, because such exclusion could conceivably enable the larger companies to exercise their market power in a way that competitively harms the smaller competitors.

Thus, it is essential for companies involved in private blockchain networks to understand that use of a blockchain cannot offer protection from the purview of the antitrust laws—even if

President Trump has signaled an intent to promote the use of blockchain technology.

### **Key Takeaways for Companies Using Blockchain**

- *Use of private blockchains will not immunize potentially anticompetitive conduct from the antitrust laws, even if the current Trump Administration has appeared to support the use of such blockchains :* Conduct occurring on a blockchain remains subject to the same antitrust laws and enforcement as if such conduct occurred through traditional channels.

- *Identify whether the blockchain's participants include your competitors:* Exercise caution when joining a blockchain with your competitors. Blockchains with multiple market participants may be viewed as a means of competitor collaboration. If you join a blockchain with your competitors, be sure that you have legitimate reasons for participating and ensure that any collaboration or information exchanged is narrowly tailored for a particular procompetitive purpose.

- *Understand how participants can access the blockchain:* Assess whether: (1) competitors can join the blockchain at a later date; (2) access to the blockchain is conditioned on an agreement to engage in certain conduct or to refrain from engaging in certain conduct; and (3) competitors are excluded from the blockchain. If membership restrictions exist, ensure they are well-defined, documented, and necessary to achieve a legitimate purpose to avoid any group boycott issues.

*Assess the types of information stored on the blockchain:* On blockchains to which competitors have access, confirm that the shared information is not competitively sensitive, non-public information, such as cost, output, customer, or pricing data that otherwise should not be shared.

**Karen Hoffman Lent and Kenneth Schwartz** are partners at Skadden, Arps, Slate, Meagher & Flom.