Antitrust Guidelines for Companies Using Blockchain Technology

Author: Luis Blanquez

Blockchain is an emerging technology that is already changing the way companies do business. Despite its nascent and novel nature, companies using blockchain technology, as well as suppliers and end users, might still get caught in the same old anticompetitive practices subject to the antitrust laws. This practice note provides antitrust guidelines to all those involved in the blockchain world who want to avoid breaching U.S. antitrust laws.

What Is Blockchain Technology?

A "blockchain" is a decentralized, electronic register in which transactions and interactions can be recorded and validated in a verifiable and permanent way. A peer-to-peer network is where different users or "nodes" share and validate information in a database or network without the need of a centralized and trusted intermediary.

Records of transactions are stored—along with other transactions—into blocks of data that are linked to one another in a chain, creating a blockchain, which is a type of distributed ledger technology (DLT). Each ledger is tamper-proof and recorded using a consensus verification algorithm that encoded every prior block in the blockchain. 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.

With the help of Web3, blockchain technology has opened the door for companies across many industries to make more efficient, inexpensive, and secure transactions without the need for a centralized authority.

Permissionless vs. Permissioned Blockchains

There are two main types of blockchains: Public blockchains, which anyone can access, and private blockchains, which only selected users have access and can participate in the network. Permissioned blockchains are a hybrid of both, meaning anyone can access them only if they have specific permissions from the network operator.

Permissionless blockchains are publicly available and fully decentralized DLTs, which means there is no central authority involved. They allow everyone to interact and participate in the validation process because they are based on open-source protocols, providing strong security. Validators need to vote to adopt the protocols and code that become the decision-making process of the blockchain. This makes it difficult to change the blockchain behavior. Transactions are also fully transparent, and the nodes involved are almost always anonymous. They have, however, some technical restraints such as (1) less control over privacy (everyone has access to what is going on in the blockchain), and (2) lower scalability and level of performance than permissioned blockchains––mainly due to the wide scope of their verification process and the amount of information they need to process. Bitcoin is an example of a permissionless public blockchain.

Dallas
100 Crescent Ct #700 - 3425
Dallas, TX 75201
469-296-7716

Detroit
28175 Haggerty Rd
Novi, MI 48377
248-994-2221

Minneapolis
331 2nd Avenue S. #420
Minneapolis, MN 55401
612-284-5001

New York
287 Park Avenue South, Suite 422
New York, NY 10010
212-634-6861

San Diego
4275 Executive Square #200
La Jolla, CA 92037
858-964-4589
info@bonalawpc.com

Permissioned blockchains are made by a smaller pool of validators who are partially decentralized DLTs. Only few known (as opposed to anonymous) and previously identified parties can access the ledger and participate in the validation process. Participants need permission to have a copy of the ledger. Thus, even though there is no central authority involved, a small group of participants validate and share the data relevant to transactions. This means less transparency and a higher risk of collusion and abuse of market power because only few nodes manage the transaction verification and consensus process. On the flip side, privacy is stronger, and private blockchains are more scalable and customizable. They are basically used for enterprise purposes such as verifying payments between parties, managing a vertical supply chain relationship, or executing smart contracts, among many others.

This distinction between public and private blockchains is important to identify and analyze antitrust issues. But the more the blockchain technology develops, the more those differences become blurred. A combination of small permissioned blockchains with more open, wider, and decentralized ones (although sometimes still using encrypted transactions) has become a common trend. Interoperability between blockchains and existing network externalities are both expected to keep verification prices down while increasing security. Ultimately, the final configuration of a blockchain and its software code will depend on the strategy and business model selected, which is something that must be analyzed on a case-by-case basis, considering the industry and applications involved.

The same issues apply to the enforcement of antitrust laws to this new technology. That's why it is essential that companies using blockchain technology have a clear antitrust policy in place and train their key employees accordingly—especially those involved with the business strategy of the company and the people interacting on a regular basis with competitors.

Potential Antitrust Issues Raised by Blockchain Technology

Anticompetitive Agreements

Fix Prices, Rig Bids, or Allocate Markets and Customers

Under U.S. antitrust laws, most agreements between companies are reviewed under the rule of reason analysis. Under this analysis, antitrust authorities and federal courts balance the anticompetitive impact of an agreement against its procompetitive benefits. These same rules, however, consider "naked" agreements to fix prices, rig bids or allocate markets or customers to be the most serious antitrust violations. Such arrangements are so damaging to competition and the market that they are almost always presumed to be unlawful under a "per se" analysis, without the need to analyze their procompetitive benefits. Usually, there are none.

Companies using a blockchain are expected to compete with other blockchains and non-blockchain rivals. A blockchain may also involve a vertical relationship, where validators, for example, use the platform to sell their products or services in the retail market or require some input from a supplier. Thus, blockchains may also facilitate anticompetitive behavior in related upstream or downstream markets.

Competitors using the same blockchain should make sure not to use algorithms or protocols to fix prices, allocate markets, or raise the transaction costs of other blockchains. Private blockchains are partially decentralized and only specified parties can access the ledger and participate in the validation process. Thus, these allow for more privacy with more dynamic consensus mechanisms to validate transactions, significantly increasing the antitrust risks. For instance, validators might be able to move from a standard proof-of-work consensus mechanism and conspire to change the protocol and algorithm of a blockchain to increase prices, while at the same time limiting other blockchains' ability to compete. This could be particularly problematic if participants within a blockchain have a hard time switching to other blockchains and non-blockchain competitors offering the same applications (likely because of the validators' market power and the existence of network effects).

Dallas
100 Crescent Ct #700 - 3425
Dallas, TX 75201
469-296-7716

Detroit
28175 Haggerty Rd
Novi, MI 48377
248-994-2221

Minneapolis
331 2nd Avenue S. #420
Minneapolis, MN 55401
612-284-5001

New York
287 Park Avenue South, Suite 422
New York, NY 10010
212-634-6861

San Diego
4275 Executive Square #200
La Jolla, CA 92037
858-964-4589
info@bonalawpc.com

Also, the risk for blockchain participants to find out the real identity of others––when such participants are competitors––and collude on prices or output restriction, increases significantly. This is particularly true when combined with the lack of visibility and access from anyone else outside the blockchain. The Department of Justice has made very clear that, similarly to traditional anticompetitive agreements, the use of computer algorithms (as is the case with blockchains) to set prices among competitors is also considered a serious violation of U.S. antitrust rules. Setting up other mechanisms such as parity or most-favored-nation clauses, although less problematic, may also increase antitrust risk for blockchain participants.

Highly decentralized permissionless blockchains, on the other hand, are less likely to give rise to price-fixing and market-allocation arrangements. All transactions are collectively taken under consensus and verified by several unknown validators who have no power individually. But when the validation process of a public blockchain loses its decentralized nature, a validator (or pool of validators) may try to acquire more capacity and as a result change the protocols of the blockchain. This could result in more control to raise prices or restrict output, either unilaterally or through a conspiracy.

The first blockchain antitrust decision was United American Corp. v. Bitmain, Inc., 530 F. Supp. 3d 1241 (S.D. Fla. 2021). The court dismissed Section 1 claims alleging mining pools, developers, and exchanges colluded during a Bitcoin Cash hard fork. The complaint failed because plaintiffs did not properly allege a plausible conspiracy across the groups or a defined relevant market. They alsodidn't show antitrust injury—the fork produced more cryptocurrency choices, not fewer.

A different result followed in In re Tether and Bitfinex Crypto Asset Litigation, 576 F. Supp. 3d 55 (S.D.N.Y. 2021), where the court sustained most Sherman Act claims alleging a conspiracy among Tether issuers and the Bitfinex exchange to inflate Tether's supply and use the new tokens to drive demand for other cryptocurrencies. Class certification briefing closed in early 2025. The case shows that coordinated volume manipulation through a stablecoin can survive Twombly without a direct price-fixing agreement on the cryptocurrency itself and could expand exchange-level collusion theories in this market.

Improper Sharing of Competitive Sensitive Information

Price-fixing agreements are not the only arrangements blockchain participants should avoid. The improper exchange of competitively sensitive information within the blockchain––especially when shared with other network participants who also happen to be competitors or potential competitors––may result in unlawful coordination. The same blockchain participants may also coordinate with other rivals from outside the blockchain itself (either blockchain or non-blockchain competitors) and share competitively sensitive information that affects prices or restricts output in a specific product market or application.

But these exchanges are not presumed to be "per se" unlawful and are usually analyzed under the rule of reason, balancing their anticompetitive impact, if any, against their procompetitive benefits. This requires a case-by-case analysis, which is based on different factors such as (1) the characteristics of the market––whether it involves competitors, together with the degree of concentration and transparency; (2) the frequency and market coverage of the information exchanges; and (3) the characteristics of the information being exchanged, notably its age (e.g., current or historical), its aggregated or individualized nature, and its strategic nature, among others.

Thus, for example, a private blockchain with few competitors where they exchange competitively sensitive information, may lead to a collusive agreement that is easy for its participants to monitor and retaliate in case of deviation. Monitoring for procompetitive reasons, such as free riding, is expected in any business industry. There is nothing wrong with that. But blockchain participants may also use smart contracts to establish automatic mechanisms to punish competitors if they decide to deviate from a collusive agreement. In case of tacit collusion in concentrated markets, such coordination might not even be necessary. And these include not only horizontal collusive agreements among competitors, but also vertical restraints in a supply contract upstream, or a retail one downstream, allowing any deviation from pricing limitations or exclusivity agreements to be easily detected.

Dallas
100 Crescent Ct #700 - 3425
Dallas, TX 75201
469-296-7716

Detroit
28175 Haggerty Rd
Novi, MI 48377
248-994-2221

Minneapolis
331 2nd Avenue S. #420
Minneapolis, MN 55401
612-284-5001

New York
287 Park Avenue South, Suite 422
New York, NY 10010
212-634-6861

San Diego
4275 Executive Square #200
La Jolla, CA 92037
858-964-4589
info@bonalawpc.com

The best way to eliminate antitrust risks among competitors when sharing competitively sensitive information in a blockchain is to avoid such exchange in the first place. If that's not possible, blockchain participants should at least encrypt any sensitive data and restrict its access within each participant exclusively to key employees not involved in pricing or business strategic decisions.

Algorithmic information-sharing is the hottest area in this space, and the case law is dividing along a single fact pattern: did the software pool nonpublic data from competitors and feed it back into pricing recommendations, or did each defendant just license the same product?

The cases that survived motions to dismiss pleaded the former. In In re RealPage, Inc., Rental Software Antitrust Litig., 709 F. Supp. 3d 478 (M.D. Tenn. 2023), plaintiffs alleged landlords fed RealPage their proprietary commercial data knowing competitors would do the same, and that RealPage used the pooled inputs to generate rental recommendations to all of them. Parallel conduct was inferred from a critical level of adoption that changed pricing strategy across the industry. The court treated the arrangement as a plausible hub-and-spoke conspiracy. The Western District of Washington reached the same result in Duffy v. Yardi Sys., No. 2:23-cv-01391-RSL (W.D. Wash. Dec. 4, 2024), where the software worked only if each defendant divulged confidential pricing information and de-prioritized occupancy in favor of algorithmic outputs.

The cases that failed pleaded the latter. Gibson v. MGM Resorts Int'l, No. 2:23-cv-00140-MMD-DJA (D. Nev. Oct. 24, 2023), was dismissed because plaintiffs did not plead when defendants began using the software, which systems they used, or the acceptance rate for recommendations. Information flowed in but not demonstrably back out. Cornish-Adebiyi v. Caesars Entm't, was dismissed for the same reason: casinos provided non-public room and occupancy data, but plaintiffs could not allege the data was pooled or commingled into a common dataset against which the algorithm ran. The Northern District of California followed both rulings in Dai v. SAS Inst. Inc., No. 24-CV-02537-JSW (N.D. Cal. July 18, 2025), dismissing claims against hotels using IDeaS revenue-management software because plaintiffs showed information was plugged into the algorithm but not how that information was later incorporated into pricing recommendations to competitors.

The first relevant appellate ruling is Gibson v. Cendyn Group, LLC, 148 F.4th 1069 (9th Cir. Aug. 15, 2025). Here, the Ninth Circuit affirmed dismissal of Section 1 claims against hotels that independently licensed the same revenue-management software. These licenses imposed obligations between Cendyn and each hotel—not among the hotels—and plaintiffs did not allege Cendyn pooled competitor data into shared recommendations. Independent adoption of a common pricing tool is not a Section 1 agreement. The court treated Cendyn's role as analogous to a back-office vendor, not a vertical supply-chain participant.

Government enforcement is moving in the same direction. The DOJ sued RealPage in August 2024 under Sections 1 and 2 of the Sherman Act, then amended its complaint in January 2025 to add six major landlords. In August 2025 the DOJ filed a proposed consent decree with Greystar that does not ban algorithmic pricing outright but prohibits using tools that rely on non-public competitor data and bars participation in RealPage-hosted landlord meetings. Cortland Management reached a similar settlement with the Colorado and North Carolina attorneys general in April 2025. States are also moving. California's AB325 (Preventing Algorithmic Price Fixing Act) makes it unlawful to use or distribute a common pricing algorithm as part of a contract, combination, or conspiracy to restrain trade, or to coerce another person to adopt its recommended price.

Independent use of a common algorithm is not a conspiracy. But pooling competitors' nonpublic data and feeding it back into recommendations crosses into Section 1 risk. A permissioned network in which validators or smart contracts ingest each participant's price, quantity, or other competitively sensitive inputs and route them back into shared outputs that other participants then follow is structurally identical to the arrangements the DOJ and plaintiffs are now targeting. So, if you want to avoid any antitrust risk, keep nonpublic competitor data out of shared computation, document that the protocol does not commingle inputs, and make sure each participant's commercial decisions remain its own.

Dallas
100 Crescent Ct #700 - 3425
Dallas, TX 75201
469-296-7716

Detroit
28175 Haggerty Rd
Novi, MI 48377
248-994-2221

Minneapolis
331 2nd Avenue S. #420
Minneapolis, MN 55401
612-284-5001

New York
287 Park Avenue South, Suite 422
New York, NY 10010
212-634-6861

San Diego
4275 Executive Square #200
La Jolla, CA 92037
858-964-4589
info@bonalawpc.com

Group Boycott

Private blockchain participants may also breach antitrust rules if they exclude competitors from the blockchain without a legitimate business justification. This is called a group boycott or a concerted refusal to deal where multiple entities combine to exclude or otherwise inhibit another party. When that "concerted" boycott involves market power or horizontal control over an essential facility or resource, courts typical analyze it under the "per se" rule.

Thus, if private blockchain participants exclude a competitor from the blockchain, and (1) the DLT is a necessary infrastructure for others to effectively compete, or (2) its members enjoy market power in the market (application) concerned, they might be subject to antitrust restrictions unless they can show an objective business justification that overrides any anticompetitive harm. That's why membership rules to permissioned blockchains should always be transparent, objective, reasonable and non-discriminatory.

Similarly, blockchain participants with market power must also avoid any horizontal collusion with members from other blockchains and non-blockchains when vertically dealing with suppliers or customers. A boycott not to deal with upstream or downstream entities, without a legitimate business justification, will create risk of antitrust liability.

Exclusionary Conduct

If you—or a competitor—has a sizeable share of the market, your (or your competitor's) conduct might be that of a monopolist subject to U.S. antitrust laws. But monopoly by itself isn't illegal. Rather, a company must use its monopoly power to willfully maintain that power through anticompetitive exclusionary conduct. Thus, a monopolization claim requires the following:

•The possession of monopoly power in the relevant market––i.e., the ability to control output or raise prices profitability above those that would be charged in a competitive market –and–

•The willful acquisition or maintenance of that power as distinguished from attaining it by having a superior product, business acumen, or even an accident of history. Exclusionary or predatory acts may include such things as exclusive supply or purchase agreements; tying; predatory pricing; or refusal to deal with its rivals. These are examples; not an exclusive list.

Finally, the monopolist may have a legitimate business justification for behaving in a way that prevents other firms from succeeding in the marketplace. For instance, the monopolist may be competing on the merits in a way that benefits consumers through greater efficiency or a unique set of products or services.

Refusal to Deal

Antitrust claims for a refusal to deal with a competitor are challenging under U.S. antitrust laws. They require a preexisting voluntary and presumably profitable course of dealing between the monopolist and rival and that the monopolist's discontinuation of the preexisting course of dealing must suggest a willingness to forsake short-term profits to achieve an anticompetitive end.

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.

Applied to the web3 world, this means that the validators of a blockchain could face antitrust scrutiny only if they had monopoly power, and (1) they previously allowed a competitor access to its blockchain but later agreed to exclude that rival, or (2) they sacrifice short-term profits without a reasonable business justification. This is, of course, unlikely considering the decentralized structure of blockchains and their need for gas fees to keep validators' business profitable and the chain secured. When the validators are decentralized, they are not a single economic entity for purposes of the antitrust laws. But the risk would still differ depending on the blockchain and the level of decentralization.

A recent test case is BiT Global Digital Ltd. v. Coinbase Global, Inc., No. 5:24-cv-09019 (N.D. Cal.). BiT alleged Coinbase delisted its wrapped bitcoin product (wBTC) in November 2024—weeks after Coinbase launched its competing cbBTC—and sought over $1 billion under Section 2. The court denied a TRO in December 2024 (no irreparable harm) and indicated in May 2025 it would dismiss the complaint, finding no plausibly pleaded falsity behind Coinbase's stated reasons for delisting. The suit was ultimately dropped. The case still previews how courts will treat duty-to-deal claims against dominant exchanges that launch competing products.

Exclusive Dealing

An exclusive-dealing agreement occurs when a seller agrees to sell all or substantially all of its output of a particular product or service to a particular buyer or a buyer agrees to buy all or substantially all of its needs for a particular product or service from a particular seller. If one of the parties to the agreement is a monopolist or near-monopolist, antitrust rules may apply when the exclusive dealing agreement is exclusionary conduct used to unlawfully acquire or maintain monopoly power. This usually takes the form of a monopolization or attempted monopolization claim. An exclusive dealing claim can also arise under Section 1 of the Sherman Act for an agreement that includes one entity with mere market power (which is less than monopoly power).

Participants with market power should thus consider any exclusive relationship within their blockchain that has an exclusionary effect. This includes restrictions (1) to only use one blockchain––because companies using blockchains are expected to compete with other companies using blockchains and non-blockchain technology when they offer similar applications; or (2) to use smart contracts to impose loyalty rebates and other barriers to switch between blockchains, among many others. This could be particularly problematic if participants within a blockchain have a hard time switching to other blockchains and non-blockchain competitors offering the same applications, perhaps because of the validators' market power and the existence of network effects.

Tying

When a seller requires buyers to purchase a second product or service as a condition of obtaining a first product or service, it may run afoul of U.S. antitrust laws. This is called a tying agreement.

A typical tying arrangement is when a seller with market power for a product (the "tying" item) requires any customer buying that item to also purchase a second item (the "tied" item). The market for the tied item is usually competitive and the seller is using its market power for the first item (the "tying" item) to increase sales in the competitive market for the second item. This tying arrangement may present competitive problems because alternative sellers of the second item—the tied product—may find themselves foreclosed from competing because buyers are coerced into buying a product from the first seller because the buyers may need the product in which the seller has market power (the first product). It may be the only way buyers can obtain the second item—by also buying the first product from the seller.

Examples of this type of exclusionary conduct may include (1) conditioning the use of one blockchain for a specific application or product by restricting the use of other blockchain or non-blockchain rivals' infrastructure, or (2) to require suppliers upstream or end customers downstream to use the same blockchain for different products or applications.

Dallas
100 Crescent Ct #700 - 3425
Dallas, TX 75201
469-296-7716

Detroit
28175 Haggerty Rd
Novi, MI 48377
248-994-2221

Minneapolis
331 2nd Avenue S. #420
Minneapolis, MN 55401
612-284-5001

New York
287 Park Avenue South, Suite 422
New York, NY 10010
212-634-6861

San Diego
4275 Executive Square #200
La Jolla, CA 92037
858-964-4589
info@bonalawpc.com

Government Enforcement

Digital Asset Market CLARITY Act

Congress's pending Digital Asset Market CLARITY Act would split jurisdiction between the SEC and CFTC and define the legal status of stablecoins. The bill has stalled over a single question: whether stablecoins are deposit substitutes (banks' position) or programmable cash that should compete with bank deposits on yield and service (industry's position). Senate negotiators have proposed banning interest "for simply holding a stablecoin" while permitting activity-based rewards. The outcome will shape antitrust exposure for banks, stablecoin issuers, and the corporate Layer-2 networks built around them. A bank-shaped regime entrenches incumbents, while an open-protocol regime forces competition on the merits.

Yuga Labs – CryptoPunks (2022)

Yuga Labs, creator of Bored Ape Yacht Club, acquired the CryptoPunks and Meebits NFT collections from Larva Labs on March 11, 2022. The deal transferred ownership of the brands, copyrights, and related intellectual property to Yuga Labs. Yuga also pledged to grant NFT holders broad commercial rights, aligning CryptoPunks with its more open licensing model. The acquisition strengthened Yuga Labs' position among leading digital collectible brands.

Because the transaction involved NFT-related intellectual property and digital assets rather than a traditional corporate acquisition, it would have required the parties to assess valuation, asset aggregation, and potential exemptions under the Hart-Scott-Rodino Act. HSR applies broadly to asset and IP transfers, including exclusive rights, and may capture nontraditional transactions if thresholds are met. There is no public record of FTC or DOJ review, and as of May 2026, no agency challenge has been reported.

Dallas
100 Crescent Ct #700 - 3425
Dallas, TX 75201
469-296-7716

Detroit
28175 Haggerty Rd
Novi, MI 48377
248-994-2221

Minneapolis
331 2nd Avenue S. #420
Minneapolis, MN 55401
612-284-5001

New York
287 Park Avenue South, Suite 422
New York, NY 10010
212-634-6861

San Diego
4275 Executive Square #200
La Jolla, CA 92037
858-964-4589
info@bonalawpc.com