Blockchain Antitrust Issues Checklist

A Practical Guidance® Checklist by Hill Wellford and Evan Miller, Vinson & Elkins LLP

Hill Wellford
Vinson & Elkins LLP

Evan Miller
Vinson & Elkins LLP

This checklist outlines antitrust considerations for the use of blockchain technology. Practices involving blockchain that could give rise to antitrust risk include competitor collaborations, sharing competitively sensitive information with competitors on the blockchain, and anticompetitive mergers involving companies offering blockchain-based services.

For more background on Section 1 of the Sherman Act, which generally governs anticompetitive agreements, please see Sherman Act Section 1 Fundamentals.

Blockchain Background

A "blockchain" is a decentralized, distributed ledger that maintains an immutable record of transactions. Businesses have deployed blockchains for a variety of purposes, including to manage supply chains, track luxury goods, validate payments, assure product quality, and manage customer loyalty programs. Businesses are still developing and exploring blockchain use cases, which are likely to expand as the technology matures.

Both the Antitrust Division of the U.S. Department of Justice (DOJ) and the Federal Trade Commission (FTC) have expressed interest in blockchain technology: DOJ's staff have undergone formal training on the technology and the FTC formed a working group on the topic. The agencies are watching this technology closely and observing its effect on competition. This increased attention means that businesses should consider the antitrust risks associated with their blockchain activities.

Participating in a Blockchain

Before participating in a blockchain, whether by joining an existing blockchain or creating a new blockchain, businesses should evaluate the characteristics of the blockchain and consider how its design, participants, and function may increase the risk of violating antitrust laws.

- **Evaluate whether the blockchain is private or public.** A "private" blockchain allows only invited participants. In contrast, as the name suggests, a "public" or "permissionless" blockchain allows anyone to participate. A "permissioned" blockchain involves characteristics of both private and public blockchains, usually assigning control or authority to a limited number of participants while maintaining the public's ability to access the blockchain. Private blockchains are associated with higher levels of antitrust risk because businesses, in theory, could use them to collude, exclude competitors, and share competitively sensitive information without easy

discovery of such activities. For antitrust purposes, the risk profile for a permissioned blockchain is similar to a private blockchain; although permissioned blockchains lack secrecy, they still could be used to exclude. Businesses considering joining a private or permissioned blockchain should evaluate the antitrust risks outlined below.

- **Identify whether the blockchain's participants include your competitors.** The "distributed" nature of a blockchain typically means that all participants will have access to all the information stored on the blockchain. In other words, businesses may use blockchains as a tool to share information. From an antitrust perspective, a blockchain in which multiple competitors participate could be treated as a competitor collaboration. Accordingly, businesses should exercise caution regarding what information is shared with their competitors (discussed in greater detail in the fourth bullet) and for what reasons. Businesses should have a legitimate reason for participating in a blockchain with their competitors, and the collaboration should be narrowly-tailored to achieve that purpose. For background on the antitrust risks of competitor collaborations, see the practice note Competitor Collaborations.
- **Learn how new participants can access the blockchain.** Businesses will want to learn (i) if their competitors can access the blockchain at a later date, (ii) whether access to the blockchain is conditioned on an agreement to engage in anticompetitive conduct, or (iii) if competitors are excluded from the blockchain for anticompetitive reasons. All of these could increase the risk of antitrust violations. For more information on when excluding competitors can create antitrust risk, see the practice note Group Boycotts or Concerted Refusals to Deal.
- **Assess what information is stored on the blockchain.** The information recorded on a specific blockchain is customized to that blockchain's purpose. For example, a blockchain designed to track the authenticity of luxury goods likely would record the provenance of the end product and its source materials. If the blockchain's participants presently include (or could include in the future) a business's competitors, it should confirm that the information recorded on the blockchain is not competitively sensitive information. This generally includes non-public information that competitors could use to make development or pricing decisions, including costs, supply, and customer pricing. For background on the risks of sharing information with competitors, see the practice note Exchanges of Competitively Sensitive Information.

After deciding to participate in a blockchain, businesses should pay close attention to its operation to ensure that changes to the blockchain's participants or governance structure do not increase antitrust risk.

- **Assess whether changes to the blockchain increase antitrust risk.** Businesses should monitor whether competitors have joined the blockchain and reassess the risks associated with competitor collaborations, specifically information sharing.
- **Do not condition access to blockchain on engaging in anticompetitive conduct.** Businesses should not operate or participate in private or permissioned blockchains that condition access on agreements among competitors to fix prices or output, or to allocate customers or markets. For background on the antitrust risks (typically severe) of fixing prices or allocating customer or markets, see the practice note Horizontal Restraints.
- **Do not exclude competitors.** Businesses should not participate in private or permissioned blockchains that exclude competitors for anticompetitive reasons.

Mergers and Acquisitions involving Blockchain

Blockchain-based services have the potential to disrupt existing industries. The agencies will pay close attention to the acquisition of a blockchain company by a competitor to determine whether the acquisition substantially lessens competition through the elimination of a nascent competitor. The agencies also may consider vertical claims if the company being acquired operates a blockchain that is essential to the acquirer's competitors such that the acquirer could foreclose competition by revoking access to the blockchain. Accordingly, businesses interested in acquiring a blockchain company should assess the antitrust risks, plan for such risk in the transaction agreement, and prepare to advocate for their deal early in the review process. For more information on how to analyze antitrust risk in mergers, see the practice note Merger Review Antitrust Fundamentals.

Hill Wellford, Partner, Vinson & Elkins LLP

Hill Wellford heads the firm's Antitrust Government Investigations team and is co-head of its HSR group. Since leaving the DOJ Antitrust Division for private practice, he has focused on matters in the energy, technology, pharmaceutical and media industries, both in the U.S. and internationally. Chambers USA calls him "very strong" in antitrust and "one to watch" (2019).

Hill's antitrust practice includes matters in the Americas, Asia and Europe. He files dozens of "merger control" notifications yearly under the U.S. Hart-Scott-Rodino Act (HSR Act) and parallel international laws, and his non-deal work includes cartel and criminal investigations, civil conduct challenges, and jury, bench, and administrative trials. He also counsels third parties involved in merger divestitures and has been appointed by the U.S. Federal Trade Commission (FTC) as counsel for agency-installed divestiture monitors and trustees.

Hill also works with the Committee on Foreign Investment in the United States (CFIUS). He assesses the deal risks of a national security review and makes voluntary and mandatory CFIUS filings, in compliance with the 2018 Foreign Investment Risk Review Modernization Act (FIRRMA) and the 2020 Treasury Department final CFIUS rules on "critical technologies" and other subjects.

Hill is a longtime leader in the American Bar Association's Section of Antitrust, where he is a member of the International Developments and Comments Task Force (IDCTF), co-chaired the Dominance Divergence Task Force that issued a landmark 2019 report, and served a three-year term on the section's governing Council. His government service included several positions in the U.S. Department of Justice (DOJ) Antitrust Division in Washington, DC, including Chief of Staff, trial attorney, investigator and Legal Policy counsel. He obtained the highest security clearances for classified information and restricted data (nuclear weapons and energy), including TS/RD. At DOJ, he also worked with the OECD, ICN, and foreign agencies, particularly focused on Asia, on matters of international trade.

Evan Miller, Senior Associate, Vinson & Elkins LLP

Evan Miller is an associate in the Complex Commercial Litigation practice group. He concentrates his practice on antitrust matters, with an emphasis on government investigations, the review of mergers by antitrust enforcement agencies, HSR filings, and civil litigation.