§11.02 An Introduction to Blockchain Antitrust

Thibault Schrepel

[A] Overview

Blockchain is to transactions what the Internet is to information. To the extent that antitrust law regulates transactions between companies, it should come as no surprise that blockchain has important antitrust implications.[1694]

Blockchain raises new competition issues. On the one hand, blockchain can be used to infringe competition law in the 'real world'. For example, two companies can collude by means of automated transactions on the blockchain (also known as 'smart contracts'). Once recorded on-chain, smart contracts are immutable which creates trust between colluders that code will enforce the terms of their illegal agreement.[1695] On the other hand, companies can infringe competition law within the blockchain. For example, miners (intermediaries who validate blockchain transactions) can divide the market among themselves to take turns validating transactions. If they do so, validation fees will rise to a level high enough level to compensate for revenue sharing.

But blockchain is also pro-competitive. When a blockchain is 'public' and 'permissionless', access to and use of the blockchain is free. All participants govern the blockchain horizontally. Such a mode of governance makes it difficult to implement of anticompetitive practices that violate Article 102 TFEU, as no single blockchain participant can implement an abuse on its own. The technical architecture of these blockchains frees economic transactions from a potential coercive power. For example, blockchain developers are guaranteed that no single user at the Ethereum (a popular blockchain) layer 1 can decide to exclude their application or impose unfair terms and conditions for access to the blockchain. In short, applications running on top of a public permissionless blockchain (e.g., decentralised metaverse) escape most leveraging practices. So much for the legal solutionists.[1696]

1694 For an in-depth analysis, *see* Thibault Schrepel, *Blockchain + Antitrust: The Decentralization Formula* (Edward Elgar, 2021).
1695 *See* Thibault Schrepel, *Collusion by Blockchain and Smart Contracts* (2019) 33 Harvard Journal of Law & Technology 117, 124.
1696 Thibault Schrepel, *Law + Technology*, Journal of Law and Technology at Texas (2023) (describing legal solutionism as 'the recasting of all complex social situations in neatly defined problems legal rules can solve').

[B] Cases

The following section provides the first comprehensive overview of the most important blockchain cases to date:

Direct Effects **Implementation**	**Anticompetitive Practice Producing Direct Effects Inside Blockchain**	**Anticompetitive Practice Producing Direct Effects Inside the 'Real Space'**
Anticompetitive practice *implemented* **inside of a blockchain**	*United American v. Bitmain* (2021); *Leibowitz v. iFinex* (pending)	Still waiting (e.g., smart contracts automating collusion)
Anticompetitive practice *implemented* **outside of blockchain**	Still waiting (e.g., a tech company cutting access to its cloud solution used by blockchain nodes)	*Gallagher v. Bitcointalk.org* (2019); National Association of Cryptocurrencies and Blockchain (2022); *BSV v. cryptocurrency exchanges* (pending)

'Blockchain antitrust' includes everything blockchain and antitrust related, regardless of whether the practices are implemented inside or outside the chain, and regardless of where their most direct effects materialise.[1697] The field is growing slowly, and while new cases are emerging, they remain limited to half of what blockchain antitrust could be. That said, recent litigation is targeting increasingly important groups and features of blockchain ecosystems.

The first blockchain antitrust case, *Gallagher v. Bitcointalk.org* (2019), involved a practice implemented outside the chain whose direct effects manifested in the so-called 'real space'.[1698] A developer sought compensation after being banned from a popular forum run by the Bitcoin Foundation. He railed against a strategy implemented to allegedly prevent him from accessing other developers and introducing a competing blockchain. The case, brought under Section 2 of the Sherman Act, was ultimately dismissed because, according to the court, 'it [was] highly unlikely that, given the opportunity, he [Gallagher] could allege cogent and viable legal claims'.[1699]

1697 The definition derives from the mindset of complexity science: including practices implemented outside the chain and/or producing their direct effects outside the chain proves crucial to understand blockchain dynamics that are *not* simply defined by on-chain practices.
1698 *Gallagher v. Bitcointalk.org et al*., 3:18-cv-05892-EMC (N.D. Cal. 2018).
1699 *Gallagher v. Bitcointalk.org et al*., 3:19-cv-01151-N-BK (N.D. Cal. 2019).

In *United American v. Bitmain (2021)*, a group of Bitcoin Cash ABC users sought relief under Section 1 of the Sherman Act.[1700] The group complained that other users had 'forked' the blockchain, i.e., duplicated the blockchain and assigned different operating rules to the new version. The group alleged that the forking diminished the value of the original chain and, because it resulted from concerted behaviour, infringed Sherman Act Section 1. The suit also targeted Bitmain Technologies, which redirected its mining power to the forked chain. The court ultimately dismissed the case for lack of evidence showing coordination with anticompetitive intent between the defendants.

In a case investigated in Brazil, the National Association of Cryptocurrencies and Blockchain (NACB) asked the Administrative Council for Economic Defense (CADE) to investigate the refusal of several banks to provide banking services.[1701] The NACB argued the refusals were anticompetitive strategies aimed at reducing the competitive pressure created by decentralised finance. The case was initially closed in December 2018 by the CADE, but the agency's tribunal requested it be reopened. The agency finally closed the case in July 2022 in favour of the banks, which justified their practice on the grounds of security and customers protection.

In *Leibowitz v. iFinex* (pending), a class action lawsuit was filed in 2020 to challenge the practices of Tether, a blockchain, and Bitfinex, an exchange.[1702] Tether's creators are accused of infringing Section 2 of the Sherman Act in the alleged stablecoin market (coins or tokens whose value is tied to an asset outside the blockchain). The plaintiffs allege that Tether released new tokens to falsely 'signal to the market that there was rapidly growing demand for cryptocurrencies' and inflate prices, while not backing those tokens with sufficient reserves. Bitfinex allegedly contributed to the scheme by allowing Tether's tokens to be exchanged for other cryptocurrencies, in violation of Section 1 of the Sherman Act. The plaintiffs are seeking compensation amounting to three times the alleged harm, i.e., approximately USD 1.4 trillion.

In a new case brought before the Competition Appeal Tribunal in August 2022 against four exchanges (Binance, Bittylicious, Kraken and Shapeshift), the plaintiff (BSV Claims Ltd.) is seeking GBP 9.9 billion in compensation for the coordinated delisting of the Bitcoin Satoshi Vision cryptocurrency. According to BSV, these exchanges colluded to damage the cryptocurrency created by Craig Wright, who has publicly claimed to be Satoshi Nakamoto – a claim he has never been able to substantiate, thus creating distrust in his other endeavors.

1700 *United American Corp. v. Bitmain, Inc.*, 1:18-cv-25106-KMW (S.D. Fla. 2018).
1701 CADE, National Association of Cryptocurrencies and Blockchain (2018).
1702 *Leibowitz et al. v. iFinex et al.*, 1:19-cv-09236-KPF (S.D.N.Y. 2019).

[C] Lessons

Several lessons emerge from these early cases. First, there are no past or ongoing cases of anticompetitive practices implemented outside a blockchain but producing their effects inside the chain. Such practices could include, for example, a tech company restricting access to a cloud solution that is heavily used by blockchain nodes. Similarly, there is no mention of cases involving anticompetitive practices implemented inside a blockchain but producing direct effects inside the so-called real space. With tens of millions of smart contracts running on public chains, the field calls for agencies to use advanced computational tools to increase detection levels.

Smart contracts pose a new challenge to law enforcement, transforming collusion from a non-cooperative to a cooperative game. Collusive agreements that do not rely on immutable code are non-cooperative, i.e., one colluder cannot force other colluders to abide by the terms of their illegal agreements. Smart contracts are different because even though they may be legally void – e.g., if they automate an illegal cartel – they will still execute when the conditions embedded in their code are met.[1703] In so doing, smart contracts make illegal agreements between companies more cooperative than before.[1704] The result is a stronger, fundamentally new type of collusion in which companies have greater confidence that other colluders will abide by their agreement.[1705] Deviations from collusive terms and leniency applications are expected to be less frequent for this very reason.

The trust that blockchain creates among users requires enforcement agencies to be more proactive in pursuing competition law infringements. One way of proceeding is to start from the so-called real space, where collusion often manifests itself (e.g., with high prices). Scanning blockchains and smart contracts in the hope of identifying illegal behaviours affecting the real space will prove more difficult, as the purpose behind blockchain transactions and smart contract code is not represented on-chain.[1706]

Second, technical knowledge is required to understand the ins and outs of antitrust cases in the ecosystem. Cases involving anticompetitive practices that are implemented and have direct effects within blockchains, such *as United American v. Bitmain* and *Leibowitz v. iFinex,* are particularly challenging from a technical standpoint. At a minimum, attorneys need to

1703 Thibault Schrepel, *Blockchain + Antitrust: The Decentralization Formula* 164 (Edward Elgar, 2021) (explores the role of oracles in executing smart contracts).
1704 *Ibid*., 165 (discusses the cooperative nature of smart contract-based collusions).
1705 *Ibid*., 138 (argues that smart contract-based collusions are more worrisome than algorithmic collusion that do not rely on blockchain, precisely because smart contract-based collusions are fundamentally new).
1706 *Ibid*., 170 (discusses concrete screening strategies for agencies).

understand the basics of blockchain to be able to communicate with the technical experts assisting them in cases.

Third, current cases involve so-called layer 1 blockchain, i.e., decentralised, distributed, and encrypted databases. Antitrust litigation has – so far – had little to do with blockchain applications such as smart contracts or Web3. One can expect litigation to increase due to exciting technical developments and increasing competition in the metaverse's space. Public enforcement may focus on the application layer, which is easier to understand and has a significant impact on consumers.

Fourth, current cases provide a glimpse into the economic significance of blockchain-related antitrust claims. Tens of millions of blockchain transactions are ordered every day.[1707] Agencies should want blockchains to remain free of anticompetitive practices that would affect all transactions ordered at higher levels. Given the current inability to detect the majority of anticompetitive practices in the real space, agencies may want to encourage blockchain adoption as a complement to antitrust. Both blockchain and antitrust seek to eliminate market coercion, i.e., decentralisation. But blockchain can only contribute if antitrust agencies supplement code where it is ineffective against anticompetitive practices. It is a great mistake to be afraid of technology when it can also contribute to our legal systems.

1707 For an overview of Ethereum transactions, *see* https://etherscan.io/.