8. Collusion on blockchain

1 WHERE WE’RE AT

Collusive agreements are consistently described as the antitrust infringement that has the most severe impact on consumers. But recent academic discussions regarding this topic appear to be missing the forest for the trees. Indeed, collusion enabled by algorithms (so-called “algorithmic collusion”) has attracted the lion’s share of policymakers’ attention. While this type of collusion may be a threat, it is much less so than collusion enabled by blockchains.

1.1 The Basics of Collusion

The antitrust literature on monopolization and abuses of dominant positions is highly polarized, as some authors dispute the harmful nature of such practices.1 There is no such debate in the literature dealing with collusive agreements. In fact, “[n]o modern development in antitrust law is more striking than the global acceptance of a norm that condemns cartels as the markets most dangerous competitive vice.”2 Cartels are regularly described as “the supreme evil of antitrust,”3 a quasi-moralist assertion around which the academic community seems to have found a point of agreement.4

Collusive agreements (i.e., agreements and concerted practices, and cartels and vertical agreements) make up the vast majority of the cases decided by the Federal Trade Commission (FTC), the Department of Justice (DOJ), and the European Commission, other than merger investigations. For instance, the

---

1 This has been especially true since the appearance of the Chicago School. See generally Robert H. Bork, The Antitrust Paradox: A Policy at War with Itself (Basic Books, 1978) (discussing the positive impact of monopolization practices on the consumer).
European Commission sanctioned zero abuses of dominance between 1991 and 2004, focusing all of its attention on clearing up the jurisprudence related to collusion. As a result, collusive agreements on both North American and European soil have been the subject of extensive case law.

1.2 Algorithmic Collusion

Recent academic research on collusive practices has focused heavily on the use of algorithms. The publication of Virtual Competition in 2016 was a pivotal moment in that regard, as it sounded the alarm about algorithmic collusion. The two authors argued that current antitrust doctrine was powerless in the face of collusion orchestrated by computer algorithms, sometimes assisted by artificial intelligence. This led to a slim academic consensus that antitrust agencies should focus their efforts on this new “supreme evil.” Yet asking for a substantial change in antitrust laws to tackle algorithmic collusion is misguided, for at least two reasons.

First, there is a lack of conclusive empirical studies documenting the phenomenon’s frequency in the actual world. In other words, the occurrence of algorithmic collusion has not been documented in official publications coming from antitrust and competition agencies, in any of the reports given to these agencies, or in the Organisation for Economic Co-operation and Development. 

---

9 Dealing, more generally, with the danger of AI, see Jamie Condliffe, “Elon Musk Implored Lawmakers to Prevent People from Building AI that Could Destroy Us All,” MIT Technology Review, July 17, 2017, https://perma.cc/QF3K-9GUW.
Collusion on blockchain

Development’s publications relating to collusion. When looking at antitrust litigation brought in the United States and Europe, algorithmic collusion is virtually non-existent. For that reason, the priority is first to quantify the phenomenon rather than drastically change antitrust and competition law. The academic community must play its part; but for the time being, cases of collusion before antitrust agencies cover agreements between individuals, not algorithms.

Second, even if algorithmic collusion became a frequent practice, it would remain old wine in a new bottle. Such collusion is a more elegant way of implementing the same anticompetitive practices that have existed for centuries. Whether or not it relies on algorithms, the nature of anticompetitive collusion remains identical. Algorithmic collusion is at the origin of two problems: detection and liability assignment. In terms of detecting illegal practices, algorithms could enable faster implementation of agreements between companies, potentially for only a few seconds. In terms of liability assignment, difficulties may arise when the algorithm whose initial order was to maximize the company’s profits decides “on its own” to collude.


13 At the time of writing, a search on the WestLawNext search engine, using “adv: ‘algorithms’ AND ‘Sherman Act § 1’”, brought up only 13 cases; hardly any concerned actual algorithmic collusion, but rather non-algorithmic collusion in which one or two companies were using algorithms in their business model. A similar search, using “adv: ‘algorithmic collusion’”, brought up zero cases.


Solutions to both of these problems are already starting to emerge. For instance, competition authorities are deploying algorithms to detect algorithmic collusion. An algorithmic antitrust battle may not be far off. As for the assignment of liability, it could be attributed to the company that is using the algorithm, to the company that created it, to individuals, or to the algorithm itself. Assigning that liability is simply a matter of legal choice. To sum up, algorithmic collusion is not yet quantified; and even if it were, it would not raise fundamental problems for antitrust law.

Antitrust and competition agencies would be well advised to focus on their resources where consumer harm can already be quantified. Unfortunately, the publication bias that pushes part of the scientific community to publish about algorithmic collusion creates a headwind and leads authorities to misdirect these resources. In the meantime, the issue of collusion by blockchain becomes ever more pressing – not because it is quantified already, but, as I shall explain, because it threatens the very foundations of antitrust enforcement.

2 BLOCKCHAIN AS COLLUSION

In this section, I study if creating a blockchain between competitors could amount to an infringement of antitrust law. I distinguish between the creation of a public or private blockchain, as this leads to different conclusions.

2.1 Public Blockchains

Can the creation of a blockchain (in itself) qualify as a collusive agreement without further analyzing the information contained within it or the use made out of it? In both the United States and Europe, I show that a public blockchain’s mere creation should not trigger antitrust or competition law interventions.

In the United States, Section 1 of the Sherman Act states that: “Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal.” The term “agreement” is not defined, but it is clear from the case law that an agreement does not need to be a formal written doc-

---


Collusion on blockchain

The United States Supreme Court held that companies enter into an illegal agreement when “the possibility of independent action” is excluded and when they exhibit “a conscious commitment to a common scheme.” Parties could meet these two criteria by agreeing to create and use a blockchain.

That being said, the exchange of public information is generally not considered an infringement of antitrust rules. In earlier decisions, the Supreme Court was concerned with such exchanges of public information, including “suggestions as to both future prices and production.” Following *United States v. United States Gypsum Co.*, in which the Supreme Court underlined that agreements to exchange information were evaluated under the rule of reason, the case law now focuses on actual evidence of anticompetitive harm. And when information is publicly available, “the risk of its exchange between competitors seems low.” Because the plaintiff bears the initial burden of proof to show that the agreement to exchange information led to substantial anticompetitive effects in a relevant market, the mere creation of a blockchain is unlikely to be seen as illegal in the United States.

In Europe, Article 101(1) of the TFEU provides that “all agreements between undertakings, decisions by associations of undertakings and concerted practices that may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition

---

25 A similar conclusion was reached in a case concerning a blockchain shipping consortium, allowing different entities to “cooperate with respect to the provision of data to a blockchain-enabled, global trade digitized solution that will enable shippers, authorities and other stakeholders to exchange information on supply chain events and documents and to collaborate with the Platform Providers on products to be offered on the Platform and the marketing of same.” The Federal Maritime Commission has declined to challenge an agreement, see “Blockchain Shipping Consortium wins Maritime Antitrust Nod,” Law 360, February 13, 2020, https://perma.cc/32Q4-ZRSF.
within the internal market” are prohibited.\textsuperscript{26} On that basis, one might ask whether creating a blockchain could amount to an agreement, a decision by associations of undertakings or a concerted practice.

The jurisprudence holds that the proof of an agreement requires:

the existence of the subjective element that characterizes the very concept of an agreement, that is to say, a concurrence of wills between economic operators on the implementation of a policy, the pursuit of an objective, or the adoption of a given line of conduct on the market.\textsuperscript{27}

One could see the creation of a blockchain by several companies as an agreement: they are indeed expressing their joint intention to conduct themselves on the market according to the information that will be contained on the blockchain and to abide by the same protocol mechanism. However, not all agreements are illegal; it depends on their nature and effects. For that reason, there is little reason to believe that the mere creation of a blockchain would constitute an anticompetitive agreement under antitrust law.

The creation of a blockchain might also be framed as a decision by an association of undertakings. But only anticompetitive decisions emanating from these associations are actionable for competition law purposes. The question is whether the mere creation of a blockchain for anticompetitive purposes may lead to intervention. Although this is theoretically possible, only a closer examination of the association’s nature and effects can provide definitive answers. One cannot conclude that the sole creation of a blockchain is therefore problematic on a general basis.

Last, could blockchain be seen as a concerted practice? According to European jurisprudence, concerted practices are characterized by the “coordination between undertakings which, without having reached the stage where an agreement properly so-called has been conducted, knowingly substitutes practical co-operation between them for the risks of competition.”\textsuperscript{28}

The CJEU further holds that Article 101 prevents direct or indirect contacts between such operators whose object or effect is to influence the conduct on the market of an actual or potential competitor.\textsuperscript{29} Interestingly, the European General Court has considered that the unilateral disclosure of information

\textsuperscript{26} Consolidated Version of the Treaty on the Functioning of the European Union art. 101(1), May 9, 2008, 2008 O.J. (C 115) 47, 88–89.


\textsuperscript{28} Imperial Chemical Industries Ltd. v. Commission, Case 48/69, European Court Reports: 1972 619 (ECJ, 1972): paras. 64–65.

\textsuperscript{29} Suiker Unie v. Commission, Case C-40/73, European Court Reports: 1663 (1975): para. 174.
relevant to the market may constitute a concerted practice, which is precisely what sharing information on a public blockchain entails. Public blockchains could also discourage companies – especially small ones – from offering different prices than competitors. As a result, provided that an anticompetitive object or effect is shown, creating a public blockchain could constitute a collusive practice in and of itself. But could such an object or effect be shown?

The Horizontal Guidelines provide that “in general, exchanges of genuinely public information are unlikely to constitute an infringement of Article 101.” The Guidelines further add that “genuinely public information is information that is generally equally accessible (in terms of access costs) to all competitors and customers”; and that “[f]or information to be genuinely public, obtaining it should not be more costly for customers and companies unaffiliated to the exchange system than for the companies exchanging the information.” This is exactly what blockchain does: it turns private information into genuinely public information. It makes markets more transparent, with all the pros and cons that entails.

European case law holds that public information sharing constitutes a cartel only when the information concerns future prices or strategies. The sharing

32 Makan Delrahim, “Never Break the Chain: Pursuing Antifragility in Antitrust Enforcement,” the United States Department of Justice, August 27, 2020, https://perma.cc/NEZ8-WC5E (“Blockchain solutions might, for instance, facilitate sharing of competitively sensitive information. As Dr. Thibault Schrepel has observed, by virtue of its distributed ledger, the blockchain ‘turns private information into genuinely public information.’ It may be difficult (or impossible) to identify which actors are sharing what information because the blockchain is based on pseudonyms and largely anonymous transactions. This combination of factors could embolden competitors to share more competitively sensitive information through the blockchain than they would otherwise”).
33 See generally Cimenteries CBR v. Commission, Joined Cases T-25/95, T-26/95, T-30/95, T-31/95, T-32/95, T-34/95, T-35/95, T-36/95, T-37/95, T-38/95, T-39/95, T-42/95, T-43/95, T-44/95, T-45/95, T-46/95, T-48/95, T-50/95, T-51/95, T-52/95, T-53/95, T-54/95, T-55/95, T-56/95, T-57/95, T-58/95, T-59/95, T-60/95, T-61/95, T-62/95, T-63/95, T-64/95, T-65/95, T-68/95, T-69/95, T-70/95, T-71/95, T-87/95, T-88/95, T-103/95 and T-104/95, European Court Reports: 2000 1531 (CFI, 2000); Aalborg Portland A/S v. Commission, Joined Cases C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P and C-219/00 P, European Court Reports: 2004 I-123 (ECJ, 2004).
34 Guidelines on the Applicability of Article 101, 92; See Cimenteries CBR v. Commission, Joined Cases T-25/95, T-26/95, T-30/95, T-31/95, T-32/95, T-34/95,
of actual prices constitutes a “market behavior which does not lessen each undertaking’s uncertainty as to the future attitude of its competitors. At the time when each undertaking engages in such behavior, it cannot be sure of the future conduct of the others.” 35 I have identified no jurisprudence sanctioning the mere act of publicly sharing actual prices because such practices do not restrict companies’ freedom to determine their market behavior independently. 36 Indeed, the jurisprudence holds that shared data must be “ultimately aimed at reducing or eliminating uncertainty about the future pricing behavior of parties.” 37 This reasoning is confirmed in the European Commission Guidelines on the applicability of Article 101 to horizontal cooperation agreements, which refer to information reducing “strategic uncertainty.” 38 In short, the data must be of such a nature that the company cannot refrain from taking it into account when defining its market behavior. 39

Evidently, the fact that public blockchains allow for information to be made public can encourage cartel creation. 40 But it also makes markets more fluid. For these reasons, it is unlikely to be considered anticompetitive. In fact, I contend that it should not be, as blockchain’s open nature ultimately helps decentralize the economy. Luckily, it is up to the Commission to show that

T-35/95, T-36/95, T-37/95, T-38/95, T-39/95, T-42/95, T-43/95, T-44/95, T-45/95, T-46/95, T-48/95, T-50/95, T-51/95, T-52/95, T-53/95, T-54/95, T-55/95, T-56/95, T-57/95, T-58/95, T-59/95, T-60/95, T-61/95, T-62/95, T-63/95, T-64/95, T-65/95, T-68/95, T-69/95, T-70/95, T-71/95, T-87/95, T-88/95, T-103/95 and T-104/95, European Court Reports: 2000 II-00491 (CFI, 2000); para. 1531 (regarding price intention); Aalborg Portland A/S v. Commission, Joined Cases C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P and C-219/00 P, European Court Reports: 2004 I-123 (ECJ, 2004). With regard to natural capacity increases, see Commission Decision 72/474, 1972 O.J. (L 303/24); Commission Decision 84/405, 1984 O.J. (L 220/27) (regarding investment plans).


38 Nicolas Petit, Droit européen de la concurrence (Lextenso, 2018): 628.

39 Discussing this point, see Izabella Kaminska, “Exposing the ‘if we call it a blockchain, perhaps it won’t be deemed a cartel?’ tactic,” Financial Times, May 11, 2015, https://perma.cc/2U4S-JTGA.
the exchange of information is the only plausible explanation of subsequent behavior’s parallelism.41 Matching that burden is complex, even though the European Commission may apply the method of faisceau d’indices (bundle of indicators).42 Indeed, similar prices or market behaviors may have numerous explanations other than collusion. Consequently, there is every reason to believe that a company sharing its current prices on a blockchain would not infringe Article 101 of the TFEU.

2.2 Private Blockchains

I now turn to private blockchains and examine whether their creation may amount to collusion. Here, one must question whether the conditions of access and use for private blockchains may be anticompetitive. These conditions are what differentiate private blockchains from public ones. The case law is clear in that matter: conditions of access can constitute an anticompetitive agreement. When the defendants have “market power or exclusive access to an element essential to effective competition,”43 the blockchain’s exclusion may constitute a concerted refusal to deal. It may also constitute market sharing if the colluders use the ledgers’ information to adapt their strategy44 (even if the information being shared is perfectly legal, but essential to operate on the market). In that regard, one may see the creation of a private blockchain as anticompetitive if its conditions of access have detrimental effects on competition.

Given this, antitrust agencies will scrutinize the creation and use of private blockchains closely. Indeed, public blockchains turn public information into private information, but private blockchains keep it private. The incentive to adapt business strategies based on private information is higher, as not all competitors can change their behaviors accordingly. Also, private blockchains would be more natural tools to share illegal information than public ones, as they are sheltered from the enforcers.

---

42 See Dresdner Bank AG v. Commission, Joined Cases T-44/02, T-54/02, T-56/02, T-60/02 and T-61/02, European Court Reports: 2006 II-3567 (CFI, 2006): paras. 64–67.
44 Here, the analysis concerns both the use and the creation of the blockchain itself.
Additionally, in Europe, exclusion from a blockchain may constitute an abuse of collective dominance,\(^{45}\) which falls within Article 102 of the TFEU. This practice is found where collectively dominant firms enjoy some structural, contractual or economic link allowing them to coordinate their behavior and act as a collective entity.\(^{46}\) One could see the decision to exclude users from a blockchain as an abuse of collective dominance. Although the case law punishing such abuses remains scarce,\(^{47}\) it could be revived. In short, antitrust agencies will, in all likelihood, keep a close eye on the establishment, use and abuse of private blockchains.

3 COLLUSIVE AGREEMENTS REGARDING BLOCKCHAINS

Blockchains could give rise to various implementations of collusive behaviors. I classify them into two categories: the agreements that concern the operation of blockchains, on the one hand; and those that concern the modification of blockchains, on the other.

3.1 Blockchain Operation

I distinguish three fundamental types of decisions relating to the operation of blockchains: decisions concerning entry into these blockchains; decisions concerning their consensus mechanisms; and decisions concerning their fee and reward structures.

3.1.1 Entry

Public blockchains are accessible to everyone by default. Any user may also become a miner or validator (the terminology differs depending on the consensus mechanism that is used) on permissionless blockchains. Therefore, it would appear that no collusive decision can be made regarding the condi-

---


Collusion on blockchain

147

tions that determine access to any of their functions. This is mostly true, but more attention needs to be paid to establishing these consensus mechanisms. Different consensus mechanisms can be put into place, and not all of them present the same degree of anticompetitive risk, as they do not require the same type of information.

Bitcoin, for example, distributes all transaction information to each user. This availability allows them to become miners by assessing the costs associated with the mining activity. This ensures a certain degree of decentralization, but it also facilitates potential collusive agreements by making these costs public.48 To this extent, one might want to provide users access to only certain types of information. But when this is the case, only one group of users decides what information is available to others. Those users thus exercise power—knowledge is power, as they say. For that reason, there is a balance to be struck when it comes to distributing the right amount of information and creating the right incentives for miners to behave properly.

Private blockchains are also interesting in that regard. Gatekeepers can choose who can access what information, which creates opportunities and risks. On the one hand, these blockchains facilitate business secrecy49 and privacy protection by removing some of the virtues of decentralization. But they also allow for the risks of cartel formation to be managed. For example, the Peruvian antitrust agency ruled in October 2020 that the creation of a joint venture between shipping companies and port operators would not be problematic (i.e., would not facilitate collusion) as, thanks to the use of a private blockchain to channel information, only the parties to a transaction would access relevant information.50 On the other hand, private blockchain holders may organize the blockchain and manage it, allowing for governing collusion when they so desire.

Last, one may want to stress that access to other facilities outside the blockchain may also raise antitrust issues. Perhaps unsurprisingly, the first blockchain antitrust case concerned a third party.51 In this case, filed in September 2018 to the U.S. District Court for the Northern District of California, the

48 Cong and He, “Blockchain Disruption”.
49 Id. at 9.
50 Informe de aprobación, prepared by Fiscalia Nacional Economica (Santiago, 2020): para. 54.
plaintiff claimed that the defendants – Bitcointalk.org, a Bitcoin developer, and the Bitcoin Foundation – were “operating an illegal monopoly.” He explained:

I have been a member of the website Bitcointalk.org since 2011 or 2012 when Bitcoin was $5 each. … I was going to be creating cryptocurrency towns. The defendants, together, used … Bitcointalk.org to deny me any ability to compete by banning me, and slandering my name even though I had 0 negative points in their reputation system.

According to the plaintiff, the practice amounted to “monopolizing the cryptocurrency technology on their website” – more specifically, to a violation of Section 1 of the Sherman Act. The case was eventually dismissed for procedural reasons, but it shows how facilities outside the actual blockchain can play an important role. For that reason, one may expect more cases of this nature to flourish in the coming years.52

Let me recall in that regard that coordinated refusals to deal are labeled as “boycotts” and are prohibited under Section 1 of the Sherman Act. Specifically, NYNEX Corp. v. Discon (1998) states that boycotts involving vertical schemes are subject to the rule of reason, while horizontal boycotts constitute per se violations of the Sherman Act (Klor, 1959). As for European competition law, the European Commission held in Papiers peints de Belgique (1974) that “collective boycott is traditionally considered one of the most serious infringements of the rules of competition, since it is aimed at eliminating a troublesome competitor. Such a boycott constitutes an intentional infringement of Article 85 (1),” now Article 101 of the TFEU. The principle has since been confirmed.53 On top of that, refusals to deal can also be sanctioned under Section 2 of the Sherman Act and Article 102 of the TFEU. I will study that in Chapter 11.

52 See, for example, in Australia, Samuel Haig, “Lawyer to File Crypto Class-Action Seeking Billions From Social Media ‘Cartel’,” CoinTelegraph, August 12, 2020, https://perma.cc/SVU6-BJ77 (accusing Google, Facebook, Twitter and YouTube of implementing a cartel intended to prevent the “burgeoning cryptocurrency sector”). In the complaint, the plaintiff argued that: “The Respondents, by their announcement and implementation of bans on advertising of cryptocurrencies and related content, have given effect to provisions in contracts, and engaged in a concerted practice, that has the purpose and has had the effect of substantially lessening competition in cryptocurrency markets in contravention of section 45 of the Act”, see Notice of Filing and Hearing, prepared by Federal Court of Australia (Sydney, NSW, July 14, 2020): para. 2.

3.1.2 Consensus
Blockchain consensus is nothing less than a blockchain’s primary rules of the game. By deciding how transactions can be validated, the consensus mechanism is at the core of blockchain’s value and integrity. Miners have the most substantial influence on it because they are bound by it at an individual level and can change it by way of a fork.

Each miner’s power is minimal on widely used blockchains where many transactions are recorded at any given time. The situation is different when miners are grouped into pools where the profit generated by the entire mining activity is shared according to each miner’s hashing power. The incentive to join such pools leads to rapid expansion. As a result, as of 2021, fewer than ten mining pools dominate Bitcoin, with just a handful validating more than 50 percent of all transactions on the Bitcoin blockchain. Because these pool miners are often physically together, it is easy to see how they could coordinate their behavior. Only a change in the blockchain’s consensus mechanism may redistribute mining power.

Although no consensus mechanism should be per se anticompetitive, some can facilitate the emergence of anticompetitive practices. Let me illustrate this by discussing two of them. Using Proof of Work, miners compete to add a set of transactions gathered as a block in the chain by racing to solve a cryptographic puzzle. The first to solve it gets to verify and validate the block and is rewarded by receiving a transaction fee and newly minted tokens. Thanks to Bitcoin, Proof of Work is currently the world’s most used consensus mechanism. It has the advantage of allowing a relatively random distribution of

---

56 For an example of miners coordinating their behavior through a pool, see Kristian Soltes, “The First Blockchain Antitrust Case. Or Is It?” Constantine Cannon, May 29, 2019, https://perma.cc/NG3X-S3LS.
58 Do miners and/or validators form a single economic entity? If that is the case, they are not separate undertakings and, as a consequence, there is no possible collusion between them. See Ioannis Lianos, “Blockchain Competition,” CLES Research Paper 8/2018 (2018): 84.
block validation operations, but encounters scaling issues due to the power that mining requires and scaling issues. Pools capture most of the mining activities, presenting concerns regarding potential collusion between them. One could also imagine that the leaders of pools may sometimes want to coordinate their behavior. Thus, the Proof of Work consensus mechanism fails to protect Bitcoin and other blockchains from collusive agreements that could ultimately lead to a change in consensus.

Under Proof of Stake, soon to become Ethereum’s consensus mechanism, each user’s chance of validating blocks increases with the number of tokens that he owns. A user with 200 tokens will be twice as likely to be selected as another user with 100 tokens. There is no coin creation (mining) in Proof of Stake, so validators are typically rewarded in transaction fees. Once a block is created, it must be committed to the blockchain. Different systems are used: some choose a random group of signers, while others require a majority. Overall, there is a risk that, by identifying the largest token holders, one could attempt to collude with them. Nonetheless, it appears more complicated than identifying mining pools with the most significant hashing power under Proof of Work. Also, while someone could rent computing power and therefore become a powerful miner, the renting of tokens is more unlikely.

Overall, one point emerges from all this: the risk of collusion is high when miners or validators are big players, and especially when the community can identify them. Blockchain participants may bribe them, or they may coordinate among themselves. Conversely, the risk of collusive agreements is much lower when the miners and validators are chosen randomly. Of course,

---


63 Amy Castor, “A (Short) Guide to Blockchain Consensus Protocols,” CoinDesk, March 4, 2017, https://perma.cc/ER9Q-824B (“In Tendermint, for example, every node in the system has to sign off on a block until a majority vote is reached, while in other systems, a random group of signers is chosen.”)

64 Large mining pools are easily identifiable on the Ethereum blockchain. At the time of writing, they are Ethermine, Sparkpool, Nanopool and F2Pool_2. They represent more than 70 percent of the Ethereum mining activity, see Etherscan, https://etherscan.io.

65 For a description of the whale problem, see “Thought Bitcoin Had a Whale Problem? Ethereum is Much Worse,” LongHash, August 27, 2018, https://perma.cc/7TZ2-VARV.

selecting them on a truly random basis may compromise the blockchain’s integrity by entrusting power to potentially malevolent participants who have little to lose. Regulatory agencies will be required to consider that balance when studying new consensus mechanisms in the years to come.

### 3.1.3 Fees and rewards

Transaction fees are essential to the integrity of many blockchains. By creating a reward for miners, they encourage them to verify transactions correctly. Some blockchains do not use any fees and seek to ensure their integrity differently. The endgame is always to prevent double spending of the same token.

As far as the Bitcoin blockchain is concerned, transaction fees are a combination of a minimum fee directly related to the transaction’s size and a bounty decided by each user to reward miners for validating their transaction faster. With the Ethereum blockchain, the fees result from a similar system, using a so-called “gas” mechanism that allows for higher than minimum fees. By contrast, private blockchains rarely use transaction fees. Integrity is, in principle, ensured by a gatekeeper. For example, Hyperledger does not use fees; validation is reached “post consensus.” The R3 Corda blockchain also works with a no-charge system, where each transaction is validated based on transaction uniqueness.

A question then arises: which mechanism presents the most anticompetitive risks? And can these fee structures be the manifestation of an anticompetitive practice? The answer is positive. Let us imagine that two blockchain nuclei agreed to change the rules for calculating transaction fees in another blockchain and attack that blockchain for the purpose (by devoting computational power). This would amount to a collusive agreement. The same would apply if two nuclei agreed together to change their own calculation rules in an identical fashion. In both cases, the decision would produce an effect outside a single blockchain. This explains why it could qualify as an anticompetitive practice.

Things are different should participants simply agree to change the rules for calculating the fees of a blockchain in which they participate. Here, regardless of the issues related to legal fictions, new rules affect all the participants. One could show the existence of an agreement leading to their implementation, but showing anticompetitive effects would prove difficult. Indeed, changing the rules implies validation by a majority of participants. One could think that they would refuse to implement new rules against their own interest. There is,


67 This is described as being “market-based” in the Ethereum white paper: 27, https://perma.cc/ZTR8-8PUF.
therefore, is a strong presumption that new rules will produce a positive effect for most of the community if they are implemented — therefore exempting them from antitrust scrutiny. In a nutshell, decisions that are internal to only one blockchain are simply neutral (or pro-competitive) business strategies.

3.2 Blockchain Modification

I distinguish three fundamental types of decisions related to the modification of blockchains: decisions that concern the core client; decisions to generate a fork; and decisions that affect the application level. Not all of them create a significant impact on other participants and blockchain layers. For example, the concentration of mining activities – often used as an example to show that blockchain is not decentralized\(^{68}\) – does not significantly affect blockchain’s use. It follows that these different types of potential collusion must be analyzed in the context of blockchain’s entire ecosystem (with its different layers).

3.2.1 Core client and developers

As we have already seen, the client’s code – running on top of the database layer – is key to blockchain’s fourth level (infrastructure). Its design is essential because it allows for more or less coordination between the core developers. This is all the more important given that the developers working on the blockchain’s core software are usually small groups with a great deal of power over the network, as I have previously explained. The Bitcoin Foundation\(^{69}\) and the Ethereum Foundation\(^{70}\) are two such groups. Their mission is to promote and ensure core client integrity. The same goes for private blockchains such as Hyperledger and R3, as they have corporate members that fund them and contribute to the code according to well-established governance structures.\(^{71}\) In short, the number, interest and location of these developers are often concen-

---

\(^{68}\) For example, see Elon Musk, (@elonmusk), May 16, 2021, https://perma.cc/ HR2Z-VS8V (“Bitcoin is actually highly centralized, with supermajority controlled by handful of big mining (aka hashing) companies”). As we saw in Chapter 7 (with the “blockchain power game”), calling a blockchain centralized because the mining power is concentrated in the hands of a few is inaccurate, as miners cannot capture the entire decision-making process or size a power of command and control.

\(^{69}\) See the Bitcoin Foundation, https://perma.cc/S2UM-GWLU.


Collusion on blockchain

trated, which often gives them the ability to steer changes. However, these core developers (e.g., Bitcoin’s and Ethereum’s) are rarely granted the power to impose changes on the client. Thus, all modifications require a majority of these blockchains’ participants.

Against this background, one should establish which agreements between core developers could amount to violations of antitrust law. First, they may propose changes whose effects are not directed inside the blockchain, but outside of it. They may, for example, want to change the code to create an agreement with another blockchain. In these situations, two legal fictions are involved. Here, antitrust law could be infringed, although one should mention that such modifications will improve blockchains in a majority of cases. Second, modifications can produce effects only within the blockchain. When the goal is to increase blockchain survival, one could consider that it benefits participants inside the blockchain. Antitrust law would thus not apply. Instead, when the modification is not intended to maximize blockchain survival, one could attribute it to participants outside the blockchain nucleus. It could then infringe antitrust law. Antitrust agencies will be tasked with identifying such agreements and their effects. That implies understanding how they can be implemented – from a technical perspective – and how coercive they are. And third, modifications can produce a “mixed-bag” effect, ensuring blockchain survival while creating a negative effect outside of it. Agencies will then be tasked to analyze whether this negative effect was strictly correlated to the chosen strategy for maximizing survival.

When it comes to public blockchains, core developers can use different means to get in touch with miners and nodes regarding future changes to the blockchain. Bitcoin uses Bitcoin Improvement Proposals (BIPs), a mechanism that allows core developers to probe miners about technical changes. The developers propose a modification and the miners express their agreement by raising “flags.” The more computing power a miner has, the more flags they have at their disposal. A general position on the blockchain thus emerges and the modification can be adopted or rejected in this way. Other times, BIPs

---


activate automatically thanks to the signaling of a majority of miners, with no “voting.”

Similarly, Ethereum uses Ethereum Improvement Proposals. Ethereum developers also use Ethereum requests for comments to discuss these proposals before putting them to a vote. Here again, coordination is made possible between developers and anyone accessing the forum. Antitrust agencies will, without a doubt, monitor the exchanges allowed by these mechanisms. Last, let me underline that one can use all forms of communication available after real-life identities are identified. The “Awemany episode,” which I described in Chapter 1, illustrates core developers’ ability to make the right phone call to the relevant mining pools.

As for private blockchains, the risk of collusion regarding the core client is even greater. While no one can force participants to use a specific core client in public blockchains (economic incentives direct them toward a single one), things are different with private blockchains, where the gatekeeper can impose one client on all participants. Further, the gatekeeper retains the ability to amend the core client. It can implement a change, for example, after consultation with specific participants only. Where such power exists, one may easily see how unilateral interventions create control over the blockchain, which could ultimately prompt collusive agreements when a few blockchain participants are involved in deciding the change or unilateral conduct when only one participant is changing the consensus.

One recent case illustrates the anticompetitive potential of modifying one blockchain core code. In late 2019, four lawsuits were filed by crypto investors over alleged manipulation of the cryptocurrency Tether and the exchange Bitfinex. Consolidated in January 2020, these actions relied on an academic paper first published in 2018 by John M. Griffin (University of Texas at Austin) and Amin Shams (Ohio State University). They argued that Tether and Bitfinex had coordinated to manipulate the price of Bitcoin.

According to the plaintiffs, Tether issued 2.8 billion tether tokens between 2017 and 2018 with the ambition to flood the Bitfinex exchange while falsely pretending that U.S. dollars fully backed its tokens (a stablecoin, i.e., a cryptocurrency designed to minimize volatility). The defendants used this unbacked

76 Id. at 29.
79 Leibowitz et al. v. iFinex et al., 1:19-cv-09236-KPF (S.D.N.Y. 2019): point 87 (“Until February 2019, Tether was saying on its website that all USDT (its token) were ‘backed 1-1 by traditional currency held in our reserves. So 1 USDT is always equivalent to 1 USD’”).
Tether (“USDT”) to purchase Bitcoin, which led to artificial pricing in the cryptocurrency market, as it allowed Bitfinex and Tether to wrongfully “signal to the market that there was rapidly growing demand for cryptocurrencies.”80 The bubble eventually burst and $466 billion in value was lost in less than a month. The plaintiffs are asking for over $1.4 trillion in (treble) damages.

The plaintiffs are introducing eight causes of action, one of which concerns antitrust laws and, more specifically, Section 2 of the Sherman Act. According to the plaintiffs, Tether controlled at the time “more than 80% of the market for stablecoins in the United States and the world. Tether therefore ha[d] monopoly power.”81 On that basis, the plaintiffs argue that the “issuance of unbacked USDT was designed to gain greater market share so Tether could eliminate stablecoin competition and maintain pricing control over the bitcoin and cryp-


Figure 8.1 Cryptocurrency bubble between 2017–18

80 Leibowitz v. iFinex, Case 1:19-cv-09236-KPF: point 6. According to the plaintiff, “half the growth in the cryptocurrency market was driven by Bitfinex and Tether’s manipulative scheme”, see Leibowitz v. iFinex, Case 1:19-cv-09236-KPF: point 11.
81 Leibowitz v. iFinex, Case 1:19-cv-09236-KPF: point 273.
This supposed monopolization practice “inflate[d] one of the largest bubbles in history.”

While the definition of the relevant market remains to be debated, and the merits of the practices should be analyzed in the light of numerous (and contrary) proofs, one can already draw several lessons from this case.

The first lesson concerns the subject matter. The first blockchain antitrust cases – known to date – all concern cryptocurrencies, showing that for now, the field is still very much focused on blockchain 1.0. The second lesson concerns the ability to manipulate blockchain, or, at the very least, to influence its value. But one should nonetheless underline Tether’s very particular infrastructure, allowing only a few users to decide among themselves the creation of new tokens. This indicates the necessity to study the “power game” within each blockchain – which implies understanding the norms, the market, the law and the digital architecture on a case-by-case basis, and how interactions between blockchain participants may influence them.

The third lesson is the ability to apply antitrust law when the identities of blockchain participants are public, and when powerful analytical tools are used to detect potential practices. The academic article which led to this case studied “over 200 gigabytes of transactional data from over ten different sources.” Performing such an analysis requires specific methods and means. Future cases concerning blockchain 2.0 and 3.0 – where the identity of transactions is not strictly financial – will not only require even more sophisticated means, but will call for regulators to cooperate with blockchain communities to enforce the rule of law. The fourth and final lesson relates, once again, to the necessity to think of antitrust law and blockchain together. As one can see, and regardless of the merits of this particular case, blockchain is an infrastructure that does not prevent all (potential) anticompetitive practices by itself (regardless of the merits of that particular case). It needs antitrust law.

---

82 *Id.* at point 276.
83 *Id.* at point 107.
84 To follow the docket activity, see *In re Tether and Bitfinex Crypto Asset Litigation*, Case Number 1:19-cv-09236, in the U.S. District Court for the Southern District of New York.
86 See Chapter 3.
87 See Chapter 7.
88 *Leibowitz v. iFinex*: point 128.
3.2.2 Forks
Not all modifications to the rules of a blockchain result in surviving forks. Some are adopted by the entire blockchain community, but a large majority are rejected. Forks are dangerous from an economic standpoint, as they can divide the value and usefulness of the blockchain. This is one important reason why blockchain communities want to avoid them, generally speaking. Only exceptionally will both chains become valuable in the long run – this is what happened with Bitcoin and Bitcoin Cash, or Ethereum and Ethereum Classic. In most situations, one of the two chains will be abandoned, along with all the transactions recorded on it.89

Authorities should pay close attention to forks resulting from an external group trying to weaken a blockchain. One can easily imagine a group of blockchain participants reducing the competitive pressure by forking a competing blockchain before abandoning it. Antitrust law will apply to these situations. Conversely, a fork that stems from a blockchain’s own participants and proves to be genuinely viable cannot be qualified as an anticompetitive practice. It results from the desire of a portion of that blockchain community to ensure long-term survival by modifying the rules.

A recent case at the border of these two strategies helps understand the underlying logic. In United American Corp. v. Bitmain, the U.S. District Court for the Southern District of Florida had to decide on the legality of a fork from the Bitcoin Cash blockchain. What happened? In August 2018, a change was proposed to allow the blockchain to accept larger blocks, which had the advantage of speeding up the validation of transactions and facilitating the blockchain’s scalability. Bitcoin.com mining pools supported this change. Another fraction of that blockchain – which included United American Corp. – opposed the move, pointing out that only a few miners would then have the necessary capacity to validate the new blocks (as they would require significantly more computing power).90

The change was implemented on November 15, 2018. Within minutes, Bitmain Technologies redirected its mining power toward the validation of


90 Discussing how to balance these interests, see Vitalik Buterin, “The Limits to Blockchain Scalability,” Vitalik Buterin’s website May 23, 2021, https://perma.cc/6K2S-9455 (underlining that “[i]t’s crucial for blockchain decentralization for regular users to be able to run a node”).
blocks following the new rules. The objective, it seems, was to surpass United American Corp.’s mining power and thus to motivate a majority of users to join the new chain. It succeeded a few hours later and implemented a mechanism for “locking down” the blockchain immediately afterward.91

The plaintiff argued that Bitcoin.com had conspired illegally with Bitmain Technologies by renting its mining power to take over the blockchain.92 The district court dismissed the initial complaint in February 2020, and in April 2021, found that because of the absence of evidence showing coordination between Bitcoin.com and Bitmain, Section 1 of the Sherman Act had not been violated.93

Supposing here that Bitcoin.com had indeed rented Bitmain Technologies’ computing power, and conspired against United American Corp., the plaintiff would have had the burden of proving that the agreement had actually been implemented to harm the blockchain and reduce its chances of survival. Put another way, United American Corp. would have been required to show that the fork was made to benefit some users only. This would have been difficult to prove. In the absence, and because antitrust law does not protect competitors

91 According to the plaintiff, “The decision by Sechet, Chancellor and Cox to ‘lock down’ the block chain after an arbitrary number of blocks close to the tip of the block-chain – through a mechanism referred to as ‘checkpoints’ and ‘Deep Reorg Prevention’ – will allow anyone with 51% hashing power to quickly cement control of the block-chain ledger. They would also cement control over future changes to Bitcoin Cash functionality as well as changes to the consensus rules. Combining this checkpoint power with the hashing power of Bitcoin ABC backers like Ver (through Bitcoin.com) and Wu (through Bitmain Technologies’ mining pools, AntPool and BTC.com) amounts to centralization. Anyone who combines hashing power and checkpoints in this fashion will be able to override any consensus reached by the rest of the network, forcing others to conform or create an unwanted hard fork,” see point 90 of the amended complaint.

92 For Ethereum, a similar question would include renting “tokens” rather than computing power. On that, see Vitalik Buterin, “On Collusion,” Vitalik Buterin’s website, April 3, 2019, https://perma.cc/FE58-ZVJY (“there’s an even cheaper attack than buying donuts (an attack that can be thought of as a kind of obfuscated bribe): renting them. If an attacker is already holding ETH, they can use it as collateral on a platform like Compound to take out a loan of some token, giving you the full right to use that token for whatever purpose including participating in votes.”)

93 United American Corp. v. Bitmain, Inc., 1:18-cv-25106-KMW (S.D. Fla. 2021), Order Granting Defendants’ Joint Motion to Dismiss First Amended Complaint (“As noted, defendants’ allegedly unlawful conduct fits into neither a horizontal, vertical nor hub-and-spoke restraint of trade paradigm …”. “After a painstaking review of the Complaint, the Court concludes that it lacks facts that create a reasonable expectation that discovery will reveal evidence of illegal agreement.”) The final judgment was issued on April 7, 2021.
or economic agents, no infringement to Section 1 of the Sherman Act would have been found despite the proof of an agreement.94

In any case, this litigation helps understand why blockchain and antitrust must be thought of together and not in silos. For example, had the Court concluded on the basis of that case that all forks are illegal (because, after all, they are agreements reducing the original blockchains’ value), this would have deprived blockchain communities of an essential feature: the possibility to exit the blockchain and compete with it. And, at times, forks are also essential to fix bugs in the blockchain core code (or improve it) and therefore make it a better infrastructure. In short, courts and agencies must keep in mind that, because blockchains are overall beneficial to consumers, practices within them must be analyzed with the intention to preserve the technology. *Per se* rules and other prohibitions related to blockchain’s essential features should be avoided for that reason.

### 3.2.3 Applications

We have already seen that blockchain’s ecosystems are built on different interrelated layers. For that reason, whoever wants to study blockchain’s sixth level – that is, applications – must do so in the context of the entire ecosystem and its key characteristics. The famous “The DAO” incident neatly illustrates why looking at this broader picture is so important.

On June 17, 2016, someone discovered a vulnerability in the smart contract governing The DAO, a decentralized autonomous organization.95 It had been exploited by one user who seized over 3.6 million Ether; but thanks to The DAO design, these tokens had been frozen for 28 days before being transferred permanently. A debate ensued within the Ethereum community regarding the creation of a blockchain fork in which one would modify the smart contract to retransfer all the stolen Ether before the deadline. A vast majority of the Ethereum community answered in the affirmative, allowing them to fork the blockchain successfully, and withdraw the funds.96

This episode is interesting insofar as a blockchain application – here a smart contract (blockchain 2.0) – has been modified at a lower level. This shows that blockchain’s immutability also applies to that level. In The DAO case, blockchain participants had no choice but to (re)transfer the funds rather than cancel...
the original transfer. To what extent can this constitute an illegal agreement? Here again, when the practice takes place within the nucleus to protect the blockchain, it escapes antitrust, as it results from a single entity. The situation is quite different when it results from the anticompetitive intention of a group of users who do not intend to ensure the blockchain’s survival. In such cases, the practice is not implemented within the blockchain nucleus, and therefore is not protected by that legal fiction. This opens the door to antitrust enforcement.

4 CHAPTER SUMMARY AND BEYOND

In this chapter, I first examined whether the creation of a blockchain could, in itself, amount to a violation of antitrust laws. This seems unlikely as far as public permissionless blockchains are concerned. Conversely, the design of private blockchains could lead to the creation of an anticompetitive cartel, depending on the parameters.

I then analyzed the extent to which the running of blockchains could amount to anticompetitive collusion. More specifically, I examined practices regarding the operation or the modification of blockchains. I explained that the day-to-day operation of a blockchain might lead to coordination and raise antitrust issues. This coordination includes decisions about the entry into a blockchain, the consensus mechanism and the calculation of fees. When it comes to modifying a blockchain – changes to the core client, the implementation of a fork or practices impacting applications – I explained that courts and agencies should distinguish between internal and external practices. The former, which are implemented by the blockchain nucleus, should be deemed legal. The latter could infringe antitrust. The distinction between public and private blockchains has proven central to my analysis.

So far, I have analyzed practices that mainly affect blockchain ecosystems. In the next chapter, I turn to practices where blockchains are anticompetitively used in a way that directly impacts the “real space.” Here, the distinction between public and private blockchains also proves to be crucial, but for a different reason: the governance it allows.