11. Blockchain and monopolization

1 PRACTICES RELATED TO BLOCKCHAIN ITSELF

This first section focuses on unilateral practices that are directly related to the blockchain infrastructure and governance. I have decided not to study practices at the application layer, as they resemble those outside blockchain. For the rest, Figure 11.1 helps identify which kinds of unilateral practices are the most likely to occur, with the understanding that consumer damage must always be proven on a case-by-case basis. This figure will have to be revised depending on the evolution of blockchain technology in the years to come, but one can use it as a first canvas.

1.1 Exclusionary Abuses

An important clarification is in order before I study the exclusionary practices that could take place on blockchains. As I shall show, public permissionless blockchains do not permit the implementation of unilateral practices by a single participant. For that reason, I must make a distinction between the initial possibility of carrying out such practices and the possibility of transforming these blockchains so as to implement them. It is thus necessary to consider whether the implementation of unilateral practices is technically possible and whether participants have incentives to do so. Finally, I make no general distinction between US and European law, because antitrust rules are similar in both jurisdictions. There are, however, some discrepancies that could have important ramifications in practice, including when it comes to the legal test being applied to these practices. I do my best to mention them.

1.1.1 Refusal to deal

Economic entities routinely refuse to do business with their rivals. However, one would expect such practices to be rare in public permissionless block-

---

1 For a general overview on European refusal to deal, see Oscar Bronner v. Mediaprint Zeitungs und Zeitschriftenverlag, Case C-7/97, European Court Reports: 1998 I-7796 (ECJ, 1998); European Night Servs. Ltd. (ENS) v. Commission, Cases
<table>
<thead>
<tr>
<th>UNILATERAL PRACTICES RELATED TO BLOCKCHAIN</th>
<th>EXCLUSIONARY ABUSES</th>
<th>EXPLOITATIVE ABUSES</th>
<th>DISCRIMINATORY ABUSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refusal to deal</td>
<td>Tying</td>
<td>Predatory pricing</td>
<td>Margin squeeze</td>
</tr>
<tr>
<td>Very unlikely</td>
<td>Very unlikely</td>
<td>Unlikely</td>
<td>Very unlikely</td>
</tr>
<tr>
<td>access to public permissionless blockchains are not submitted to conditions of buying/using another product or service</td>
<td>access to public permissionless blockchain is free, and transaction fees apply the same to all participants</td>
<td>implies two majority changes, first, to adopt the lower price to use the blockchain, then to raise it</td>
<td>implies a majority change in the blockchain, despite significantly reducing its attractiveness</td>
</tr>
<tr>
<td>Privately Blockchain</td>
<td>Very likely</td>
<td>Likely</td>
<td>Very likely</td>
</tr>
<tr>
<td>refusal to give access is one of the reasons why private blockchains exist</td>
<td>access to the blockchain can be easily subjected to conditions, such as creating another account / using another blockchain</td>
<td>to date, no court or agency is imposing to grant blockchain access, removing in effect any incentive to squeeze the margins of those who have gained access</td>
<td>significantly increases the overall attractiveness and value of blockchains which have exclusive information</td>
</tr>
</tbody>
</table>

**Figure 11.1** The implementation of unilateral practices on blockchain
chains. Access to these blockchains is free by default. Should the access rights be modified to limit access, the blockchain would no longer be “public.” One could thus say that refusal to deal or grant access is inconsistent with the inherent nature of public blockchains.

By contrast, the possibility to refuse access is an essential characteristic of private blockchains. Their creators can indeed restrict entry (whether entirely or to certain functions such as validating transactions), see all information and use it as they see fit. Doing so, of course, is not necessarily illegal. In the United States, we know from *Aspen Skiing* (1985) that “[t]he high value that we have placed on the right to refuse to deal with other firms does not mean that the right is unqualified.” Although the *Trinko* decision (2017) has since reaffirmed the absence of any duty to deal with rivals, it remains unclear whether the ruling applies to all situations or solely to regulated industries.

As for European competition law, we know from *Commercial Solvents v. Commission* that:

an undertaking which has a dominant position in the market in raw materials which, with the object of reserving such raw material for manufacturing its own derivatives, refuses to supply a customer, which is itself a manufacturer of these derivatives, and therefore risks eliminating all competition on the part of this customer, is abusing its dominant position.

T-374/94, T-375/94, T-384/94 and T-388/94, E.C.R. II-3141 (1998); *Clearstream Banking AG v. Commission*, Case T-301/04, European Court Reports: 2009 II-3155 (CFI, 2009). In short, refusing to provide access to a facility is abusive if it is likely to eliminate all competition on the secondary market, if access is indispensable for entering the market in question and if access is denied without any objective justification. For an overview of American refusal to deal, see *Verizon Comm. Inc. v. Law Offices of Curtis V. Trinko*, LLP, 540 U.S. 398 (U.S., 2004), in which the court suggested that a refusal to deal motivated solely by a desire to eliminate competition, with no other purpose, might constitute illegal monopolization. To establish liability under the essential facilities doctrine, a plaintiff must show the monopolist’s control over the essential facility, the plaintiff’s inability to duplicate the essential facility, the denial of use of the facility and the feasibility of providing access to the facility.

2 The refusal to grant access to the blockchain could be an abuse of dominant position if decided by one company, but it could also be a cartel if the blockchain is run by a consortium.

More specifically, the CJEU held that a refusal to deal might be punished when: (1) it concerns an input indispensable to do business; (2) the refusal is likely to eliminate competition; and (3) it is not objectively justified. The General Court followed up with similar reasoning in Microsoft v. Commission, holding that:

the refusal by an undertaking holding a dominant position to license a third party to use a product covered by an intellectual property right cannot in itself constitute an abuse of a dominant position within the meaning of Article 82 EC. It is only in exceptional circumstances that the exercise of the exclusive right by the owner of the intellectual property right may give rise to such an abuse.

The following circumstances must be considered to be exceptional:

in the first place, the refusal relates to a product or service indispensable to the exercise of a particular activity on a neighbouring market; in the second place, the refusal is of such a kind as to exclude any effective competition on that neighbouring market; in the third place, the refusal prevents the appearance of a new product for which there is potential consumer demand.

One could easily see how these could play out in a blockchain environment: firms in a private blockchain could refuse access to it and thus eliminate competition in a downstream innovative market. This will surely happen.

Besides, there are similarities between refusals to grant access to a blockchain and refusals to grant standard-essential patents (SEPs). Concluding a license to use SEPs is deemed essential to compete on the market, because they are often integrated into norms. For that reason, the holders of SEPs are often encouraged by standard-setting organizations to license them on fair, reasonable and non-discriminatory (FRAND) terms, to avoid any breach of antitrust law. One can imagine that similar case law will be developed whereby private blockchain holders will have no choice but to grant access to their blockchains on FRAND terms if access is deemed essential to compete.

Generally speaking, should access to specific blockchains be recognized as a de facto necessity, the firms running such private blockchains would be prohibited from setting access terms that create a strong exclusionary effect. For these reasons, blockchain gatekeepers (those in control of private blockchains)

---

9 Id. at para. 332.
should carefully consider, without further ado, whether their access conditions comply with antitrust law.

The same goes for gatekeepers located outside of the blockchain ecosystem. In a recent case, a Brazilian association of cryptocurrencies operators (the National Association of Cryptocurrencies and Blockchain) asked the antitrust agency, in June 2018, to investigate Banco do Brasil’s refusal to supply banking services to these operators. In response, Banco do Brasil argued that it took precautions, and indeed refused to supply them, only to avoid any risk of financial crime by its clients.

The Administrative Council for Economic Defense initially closed the case in December 2018, but the agency tribunal asked for the investigation to be reopened in Summer 2020. The case is currently ongoing at the time of writing. Regardless of the outcome, it shows that blockchain antitrust issues also concern operators that can affect the ecosystem from the outside. Similarly, one could imagine antitrust actions against an exchange that would refuse to list a token for anti-competitive purposes.

1.1.2 Tying

“Tying” is the practice of subjecting the sale of one product (or service) to additional sales or obligations. It may, for example, involve subjecting a contract to the acceptance of supplementary obligations.

Tying is unlikely to be seen on public permissionless blockchains. This type of blockchain can be accessed or used freely; submitting it to the use of another product or blockchain is unlikely. To this extent, and given the difficulty of modifying public blockchains, it is doubtful that one would find an abundance of such practices. They would have to be incorporated into the blockchain’s

---

10 Discussing the subject, see Delrahim, “Never Break the Chain” (“consider seafood harvesters that establish a permissioned blockchain to track food through the supply chain and assure quality and sourcing. If multiple competing harvesters conditioned access to that permissioned blockchain on agreeing to certain prices or output, competition and consumers would suffer tremendous harm.”)

11 Candil, “Cryptocurrency association”.

code from the very first day. Also, such strategies can lead to a reduction in the potential number of users, which is contrary to the principal objective of public permissionless blockchains: to create network effects. Precisely because tied sales and the creation of network effects do not mix well, the modification of public permissionless blockchains to implement such practices is unlikely.

On the other hand, private blockchains may have an interest in imposing tying or similar practices. This may be the case, for example, where a company requires an account on another platform or the owning of tokens to connect to its blockchain. This might also be the case where a blockchain gatekeeper requires that certain tasks be performed before becoming a validator. Here too, the desire to implement tying practices may be counterbalanced by the intention to generate strong network effects. However, private blockchains do not entirely rely on network effects to generate value. Indeed, their functioning is more centralized than that of public blockchains (as we established in Chapter 2), and, therefore, their integrity and scalability do not entirely depend on the number of users. One may therefore expect more tying on private blockchains.

1.1.3 Predatory pricing
Attempts to drive smaller competitors out of the market by systematically undercutting them have been the subject of numerous court decisions. On blockchain, pricing occurs mainly in the form of transaction fees when a user submits a transaction to be registered into the chain. Predatory pricing is very unlikely on public permissionless blockchains, because the practice will be possible only if enough users are convinced, first, to change the governance structure to lower the price, and second, to change it back to a profitable level.

The situation is different for private blockchains. Private blockchains can change the protocol and transaction fees at any point in time without having to convince anyone to adopt the change. The pricing can therefore be changed easily in response to a competitor’s strategy. One could imagine, for example,

---

13 Id.
14 In the European Union, predatory pricing is considered abusive if the prices charged by the dominant undertaking are below average variable costs or if the prices charged by the dominant undertaking are below average total costs and they are set as part of a plan for eliminating a competitor. See France Télécom v. Commission, Case C-202/07 P, European Court Reports: I-2369 (2009). In the United States, in order to establish predatory pricing, the plaintiff must show below-cost pricing and a dangerous probability of recoupment by the monopolist once the rival has been driven from the market. See Brooke Group Ltd. v. Brown & Williamson Tobacco Corp., 509 U.S. 209, 223–24 (U.S., 1993).
a private blockchain offering its users low transaction fees to eliminate competing blockchains. The legal test for predatory pricing would then apply.

1.1.4 Margin squeeze
Margin squeeze occurs when a vertically integrated dominant company operates on upstream and downstream markets, and sets the upstream price high enough so that companies cannot compete sustainably in the downstream market. This practice, by definition, cannot be implemented on public monocentric blockchains, as they allow only one application. The same cannot be said of public platform blockchains; but because access to this infrastructure is free, the implementation of margin squeeze is hard to conceive. Raising the costs of the transaction fees for the purpose of squeezing margins also appears implausible, as the new fees would apply to all use cases.

The situation is different for private blockchains. Different transaction fees could be applied to specific participants. The gatekeepers of private blockchains could thus implement a margin squeeze strategy. While this strategy seems unlikely in the development phase of blockchains, it will become more likely as the industry matures. It should be closely monitored.

1.1.5 Exclusive dealing
Another anticompetitive practice consists in granting retroactive rebates or discounts conditional on a customer getting all or most of its goods or services from the dominant entity. One could include such terms in the user

---


17 For an overview of exclusive dealing, see Tomra Sys. ASA & Others v. Commission, Case T-155/06, European Court Reports: 2010 II-4361 (2010), and Intel Corp. v. Commission, Case C-413/14 P, European Court Reports: 2017 632 (2017). In the United States, exclusive dealing may constitute a violation of Section 2 of the Sherman Act if it forecloses competitors from accessing the market. The D.C. Circuit held that “a monopolist’s use of exclusive contracts, in certain circumstances, may give
agreement, which is signed before using the blockchain.\(^{18}\) It seems unlikely to see such exclusive dealings on a public permissionless blockchain, as, by definition, each participant may leave and rejoin the network at will, without restricting its use.

Again, the situation is different for private blockchains. Private blockchains are interested in increasing their attractiveness by obtaining data that they alone can provide. This increases the attractiveness – and the value – of the blockchain. Exclusive dealing could be easily imposed in the terms and conditions of these blockchains. The chances that exclusive dealing practices will be implemented on private blockchains are high for that reason.

### 1.1.6 Rebates and discounts

Dominant entities may also want to grant rebates and discounts in a way that is anticompetitive – that is, where this induces fidelity and hurts competition.\(^{19}\) Granting such rebates and discounts on a public blockchain would imply a major change in its infrastructure, which appears unlikely to be accepted as it would benefit only a minority of users. For example, one might want to grant a rebate for reducing a user’s costs to transact on a blockchain. This could be done by reducing the fees the user must spend for transactions to be validated. On the Bitcoin blockchain, these fees are calculated on the amount of data that makes up a transaction: the more data, the higher the fees. A rebate could be granted to reduce the fees a specific user has to pay while promising that her or his transactions will be rapidly validated.

Granting such a rebate would require giving specific users the right to change these fees, which is unlikely to be done in existing blockchains. But even where this could be done, it is important to remember that all practices are recorded and visible on public permissionless blockchains. One user’s dis-

---

\(^{18}\) For an example, see “Ethereum Foundation, Legal Agreement”, Ethereum.org, https://perma.cc/57TB-G4NU.

account would be visible to all, and the grant of loyalty rebates or discounts could lead to push-back from users that do not enjoy the same discount. This would significantly reduce the blockchain’s attractiveness. Therefore, one should not expect many of these practices on public blockchains.

Private blockchains may technically implement rebates and discounts. They also do not necessarily suffer from the “visibility effect,” which lets all users know about rebates and discounts, because they can determine what information is visible to each user. They may, in short, create the conditions for attracting reputable users by offering them discounts while keeping all others. Rebates are thus expected to arise on such blockchains.

1.1.7 Predatory innovation

“Innovation” is “the implementation of a new or significantly improved product (good or service).”20 Each time one changes the blockchain infrastructure, the modification can be described as an innovation. And where there is innovation, there is a risk of predatory innovation: “the alteration of one or more technical elements of a product to limit or eliminate competition.”21 Predatory innovation mirrors positive innovation – it is, after all, a new version of a product or technology; but it does not bring any real improvements to users. It is simply... new. In short, predatory innovation encompasses all anticompetitive strategies that aim to eliminate competition without benefiting consumers or users under the guise of improving products.

While the initial choice of a blockchain’s public or private nature should be exempt from antitrust scrutiny,22 the chosen architecture affects the likelihood of anticompetitive practices. As far as public permissionless blockchains are concerned, predatory innovation could be implemented only if a majority of the miners adopted a new governance design. This seems unlikely, as the change would hurt part of the deciding community – but not impossible. That said, any change to a public blockchain’s infrastructure requires coordination and consensus among most participants.23 Thus, as a public blockchain’s

---

23 No rule, however, is set in stone. They can all be modified with a broad consensus.
As is often the case, things are different for private blockchains. In the words of Ethereum creator Vitalik Buterin, “the consortium or company running a private blockchain can easily, if desired, change the rules of a blockchain, revert transactions, modify balances, etc.” This ability may lead to predatory innovation, where a change in the rules is easy and requires no user approval.

Predatory innovation may become a common practice in private blockchains, for several reasons. First, one can implement a predatory innovation strategy at no cost merely by changing a blockchain’s code. Its implementation can also be quick, as interactions and validations via blockchain usually take only a few seconds or minutes. And although transactions and modifications are not invisible on public blockchains, they can be on private blockchains. On top of that, predatory innovation on blockchain can have a radical effect – for example, excluding targeted users that are also competitors. Last, predatory innovation practices can take different forms with multiple effects beyond mere exclusion from the blockchain. A company that owns a private blockchain can change its governance design so that a user’s access is simply denied or so that the user can no longer read all the information on the blockchain, register transactions or take part in the block validation process. In a nutshell, predatory innovation remains one of the most expected and dangerous anticompetitive strategies that can be implemented on private blockchains.

1.2 Other Abuses

1.2.1 Exploitative abuses

Exploitative abuses entail the direct or indirect imposition of unfair conditions on existing customers or suppliers. Theoretically, these are not prohibited under US antitrust law. Still, some of these exploitative practices are sanc-


26 In fact, using a “godmode,” the private blockchain owner can freeze any account or move the funds away, but the chances are that people will eventually discover it and sell all the stocks, securities or tokens.

27 Article 102(a) of the TFEU refers to the imposition of unfair purchase or selling prices as well as other unfair trading conditions. Consolidated Version of the Treaty on the Functioning of the European Union art. 102(a), 2008 O.J.C. 115/47. See Rambus v.
tioned — sometimes under different labels — on both continents, especially when it comes to intellectual property and digital markets. As underlined by Harry First, “contrary to conventional wisdom, antitrust law is being used today to control the ability of intellectual property rights holders to exploit their licensees through excessively high prices or the imposition of particular nonprice terms.” Exploitative practices are therefore relevant in both Europe and the United States, although they remain arguably preeminent on the European side.

Blockchain’s participants should keep informed about the activities of antitrust agencies in the field. For example, the creation of a dual blockchain environment with preferential treatment (paid prioritization) — one for those who pay the most and another for those who pay less and whose transactions will lag behind — might be questioned by agencies.

These dual environments are more likely to be implemented in private blockchain environments than public ones. The imposition of differentiated terms on just a few participants will prove difficult in public permissionless blockchains, as I have previously explained. On top of that, access is free and easy, switching costs and barriers to exit are low, creating a disincentive to engage in such practices. It follows that paid prioritization, where it exists, should not be seen as being systematically anticompetitive. Ethereum is a good example. Blockchain’s participants can pay extra fees (called “gas fees”) to

---

28 See Harry First, “Exploitative Abuses of Intellectual Property Rights,” in The Cambridge Handbook of Antitrust, Intellectual Property, and High Tech, eds. Roger D. Blair and D. Daniel Soko (Cambridge University Press, 2016): 222–23, 241 (“It is the standard view in the United States that … antitrust law does not reach acts of exploitation by a monopolist … [W]ithout denying this substantial divergence in general between the United States and the rest of the world, it turns out that there may be fewer differences between the United States and other jurisdictions when it comes to judging exploitative behavior by intellectual property rights holders with market power … [C]ontrary to conventional wisdom, antitrust law is being used today to control the ability of intellectual property rights holders to exploit their licensees through excessively high prices or the imposition of particular nonprice terms.”) For cases, see Microsoft Corp. v. Motorola, Inc., 795 F.3d 1024, 1033 (9th Cir. 2015); Broadcom Corp. v. Qualcomm Inc., 501 F.3d 297, 310, 314 (3d Cir. 2007).


encourage their transaction to be validated first. This leads to the prioritization of those who pay the most, thus creating a procompetitive environment between users.

The picture is different with private blockchains. Paid prioritization can result not from a public process, but from abusive practices aimed at discouraging certain users. Fee modifications can indeed be implemented unilaterally, beyond the participants’ sight. The fact that switching costs are higher than they are in public blockchains (due to access fees and conditions) reinforces the assumption that paid prioritization could be detrimental to competition, even when the practice is known to users.

This type of abuse will undoubtedly be the subject of legal proceedings. In this regard, it is worth underlining that the rise of the term “fairness” at the European Commission—whose definition and scope are still undefined—could be seen as a sign of its willingness to tackle exploitative practices more aggressively. In an Impact Assessment, entitled “Fairness in Platform-to-Business Relations,” the European Commission identified several issues related to platforms, including the negotiation of terms and conditions. One may find several indications that a similar direction is being taken in the United States. Overall, everything suggests that antitrust agencies will tackle blockchain issues under this general policy.

1.2.2 Discriminatory abuses
Discriminatory abuses occur when parties apply “dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at
a competitive disadvantage.”36 Price discrimination is the most common of these.37 According to Judge Richard Posner:

price discrimination is a term that economists use to describe selling the same product to different customers at different prices even though the cost of sales is the same. More precisely, it is selling at a price or prices such that the ratio of price to marginal costs is different in different sales.38

Price discrimination involves favoring specific customers. In practice, it occurs in two ways: (1) charging different customers different prices for the same product; or (2) charging customers the same price for different products.

Could price discrimination occur in the blockchain space? Of course it could. But let me recall that, first, the implementation of such practices on public permissionless blockchain would require approval by the majority, which is unlikely; and, second, because of the “visible effect” of public permissionless blockchains, price discrimination would be limited as it would reduce the blockchain’s attractiveness. To be sure, one will find many instances in which different prices are charged to use the same blockchain. But so long as they correspond to different services or are applied to different users based on objective criteria, they will not be found to be discriminatory.

For private blockchains, one could easily implement discriminatory practices. Perhaps users will encounter discriminatory terms because they could help incentivize them to be active on the blockchain by offering lower prices, thus creating a potential discrimination claim for others. Once again, private blockchains will be the center of focus.


37 In European judicial history, there are few cases in which price discrimination alone was found abusive. See Clearstream Banking AG v. Commission, Case T-301/04, European Court Reports: 2009 317 (CFI, 2009) (referring to anticompetitive foreclosure when an “as efficient competitor” cannot compete effectively with the price of the dominant undertaking); see also Post Danmark A/S v. Konkurrencerådet, C-209/10, European Court Reports: 2012 172 (ECJ, 2012) (clarifying that where prices are below average total costs while being above average incremental costs, a finding of abuse requires a demonstration of actual or likely exclusionary effects). In the United States, price discrimination by a monopolist violates Section 2 of the Sherman Act only to the extent that it is predatory or otherwise excludes competitors from the relevant market. See Blue Cross & Blue Shield United of Wis. v. Marshfield Clinic, 65 F.3d 1406, 1413 (7th Cir. 1995). Price discrimination may also violate the Robinson-Patman Act. See Brooke Group Ltd. v. Brown & Williamson Tobacco Corp., 509 U.S. 209, 220 (U.S., 1993).

2 PRACTICES USING BLOCKCHAIN

In this section, I analyze the extent to which blockchains can facilitate unilateral anticompetitive practices in the real space. In this regard, it is important to distinguish practices that merely use blockchain from those that involve smart contracts. This dichotomy is similar to that which I have used in the two chapters on collusive agreements. As I show, it seems highly unlikely that such practices could be created without the support of smart contracts.

2.1 Without Smart Contracts

Blockchain could theoretically be used without smart contracts to pursue unilateral anticompetitive purposes in the outside world. In practice, however, companies will use a blockchain when the technology’s characteristics benefit their practice. Against this background, one must question whether blockchain characteristics could help abuses of dominant position. The answer seems negative.

I have shown that the immutable nature of blockchain creates trust between colluders, thus providing a technical answer to a classic cartel problem. But the same cannot be said of monopolization. Let me illustrate that claim by studying blockchain’s key characteristics: encryption and immutability (see Chapter 2 for a technical explanation).

Thanks to encryption, the identity of users and the content of their transactions on the blockchain remain secret. This creates what I have called the “opacity effect,” which complicates the detection of collusion. However, this does not protect monopolization practices with real-world impacts, as companies know the identity of their (dominant) business partners. As a result, one participant’s public key can easily be correlated with its actual life identity. The same applies for the content of transactions. Decoding the hash value of transactions is undoubtedly complex, if not practically impossible considering the limits of computing power. Still, the fact remains that abused companies can easily establish a link between the problematic blockchain transactions and the real-world identity of the abuser. Encryption is not helpful for dominant companies.

The same can be said for immutability. Monopolization practices do not require a high level of trust between different players, as is the case with collusive practices. Accordingly, there is no need to transform any relationship into a cooperative game. Thus, except in limited cases, the immutable or unstoppable nature of smart contracts is indifferent to those who want to implement an illegal practice on their own. That feature could even create a negative effect. As I have previously discussed, one may not exclude that companies
could fear their practice will be more easily discovered when implemented on a blockchain. The result is that neither of blockchain’s two principal features encourage monopolization practices. But things are different when smart contracts are involved.

2.2 With Smart Contracts

Smart contracts can be useful allies in implementing various anticompetitive practices. Let me take a step back before analyzing each one of them. I have shown that smart contracts provide an important support to cartels by generating trust. Because companies do not encounter this trust problem in monopolization settings, one can logically expect that smart contracts will foster fewer unilateral practices than collusion. Still, I will try to draw up a risk map to help identify which practices are most likely to emerge.

As I shall explain, the distinction between public and private blockchains is not as essential here as it is for unilateral practices concerning the blockchain itself (such as those I studied in the previous section). The smart contracts I am about to discuss are implemented on top of existing layer 1 infrastructures. One does not need the approval of a majority to implement them. Finally, while many of these practices could be implemented using algorithms outside blockchain, blockchain’s immutability may prove useful.

2.2.1 Exclusionary abuses

2.2.1.1 Refusal to deal
Refusal to deal or grant access often implies the absence of any contract. To that extent, explaining how smart contracts could help implement such practices might seem strange. But they can help. As we know, refusals to deal or grant access are not limited to sheer refusals. In practice, subjecting the signing of a contract to excessive (i.e., exclusionary) conditions may lead to a similar result. A dominant firm could impose such conditions on a smart contract.

2.2.1.2 Tying
A company may want to impose the use of a public permissionless blockchain when buying a product or service in the real space. In such a situation, access to the blockchain is free, but one could see the practice as a way of forcing people to use a product (here, the blockchain) they do not want. A company might also impose conditions to acquire tokens with the purchase of an independent product or service – effectively imposing additional costs on buyers. This will likely become a standard practice in the years to come, raising antitrust questions related to tying.
## Figure 11.2 The implementation of unilateral practices via blockchain

<table>
<thead>
<tr>
<th>UNILATERAL PRACTICES USING BLOCKCHAIN (WITH SMART CONTRACTS)</th>
<th>EXCLUSIONARY ABUSES</th>
<th>EXPLOITATIVE ABUSES</th>
<th>DISCRIMINATORY ABUSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public permissionless blockchain</td>
<td>Likely</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely by definition, a refusal to deal implies the absence of any (smart) contracts, but in practice, submitting the signing of a (smart) contract to excessive conditions may lead to a similar result</td>
<td>Very likely</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private blockchain</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely conditioning the sale of a product or service to the use of a specific blockchain or the purchase of tokens</td>
<td>Likely ensuring automatic price changes (first down, then up) via smart contracts, according to a set of predefined rules to exclude rivals</td>
<td>Unlikely ensuring automatic price changes via smart contracts according to a set of predefined rules (linked to the downstream price) to squeeze competitors' margins</td>
<td>Unlikely ensuring through smart contracts that a purchase is automated whenever a set of predefined conditions (indicating a need) are met.</td>
</tr>
</tbody>
</table>
2.2.1.3 **Predatory pricing**
Predatory pricing involves a two-step strategy (although only the first is required in European competition law): a price decrease below the competitive level and a subsequent price increase above the competitive level, once competitors are excluded. In this respect, the use of smart contracts could allow price changes to be performed automatically, in either direction. The advantage that a dominant undertaking might gain in using a smart contract rather than a simple algorithm is that a smart contract could be considered a legally valid sale contract (if it meets specific requirements, depending on each national law). This interaction would then be recorded in the ledger. Besides, the dominant company could use different oracles searching for information on competitors’ websites to adjust its strategy. This practice is likely to increase in the coming years.

2.2.1.4 **Margin squeeze**
As with predatory pricing, one can easily implement margin squeezes through smart contracts. Here, the dominant undertaking defines the rules of the contract in such a way that the price for access to an infrastructure (whether a private blockchain or another type of infrastructure) is a function of the price charged in the downstream market. The advantage of using a smart contract over a simple algorithm is the ability to create contracts directly through the blockchain and link different oracles to use variables on top of an immutable smart contract.

2.2.1.5 **Exclusive dealing**
Smart contracts could also automate purchases when predetermined conditions are met. For example, they could automate sending new supplies every time a company sells X number of products. One could indeed link smart contracts to inventories and ensure automatic transactions. One should nonetheless expect some reluctance from business partners to provide information promptly and grant access to their inventories.

2.2.1.6 **Rebates and discounts**
Smart contracts can also manage loyalty rebates and discounts, as they can automatically grant certain discounts whenever specific predefined conditions are met. For example, a smart contract may grant a retroactive payment when a predefined number of products have been purchased. It would allow the

---

implementation of complex rebate systems while ensuring that the parties have full visibility of the system in place, and can trust its immutability.

2.2.1.7 Predatory innovation

Smart contracts, by definition, can be used to automate tasks within blockchain. It is thus hard to imagine how they could operate changes on products or platforms located outside of it. And even if this could be done, it is hard to see why this process would be superior to implementing predatory innovation without a blockchain.

2.2.2 Other abuses

2.2.2.1 Exploitative abuses

The number of cases involving exploitative abuses is increasing.40 One should logically expect agencies to open related investigations in blockchain ecosystems.

To start with, dominant undertakings could use smart contracts to force a partner to provide an escrow which will be released depending on its behavior. The implementation of such a mechanism could be considered abusive under European competition law, as it strongly unbalances the relationship between the two companies that are parties to the transaction.

Dominant firms could also force their partners to sign pre-drafted smart contracts – so-called “adhesion contracts” (as defined at the beginning of the twentieth century by Raymond Saleilles).41 Such contracts are not illegal by default, but they can be in several European countries when both parties have not freely consented to them. Smart contracts could also impose unfair terms of this sort.42

41 Adhesion contracts are typically drafted by one party and signed by another party with lesser bargaining power, see Raymond Saleilles, De la déclaration de volonté: Contribution à l’étude de l’acte juridique dans le code civil allemand (Librairie Cotillon, 1901): 119 (defining an “adhesion contract” as a contract for which “there is an exclusive predominance of a will forcing the co-contractor to “adhere to it”).
2.2.2.2 Discriminatory abuses

As we have seen, discriminatory abuses arise when a company imposes dissimilar conditions on trading partners which are in similar situations. Smart contracts can be used to implement such practices, as they may facilitate complex and differentiated conditions. And because they are automatically executed, they eliminate a majority of the monitoring costs that one might incur for similar contracts outside the blockchain. There is thus a risk that smart contracts will be used for discriminatory ends, whether antitrust law is infringed upon signing of the contract or after several conditions are met.

3  CHAPTER SUMMARY AND BEYOND

The distinction between public permissionless blockchains and private blockchains is central to the practices impacting the blockchain itself. The gatekeepers of private blockchains hold unilateral powers, which significantly facilitates the implementation of anticompetitive practices. The presence of a pilot in the cockpit of private blockchains shows the need for antitrust agencies to focus on the latter. As for public blockchains, anticompetitive practices may be implemented only when the blockchain has allowed this from the outset (which is unlikely to be the case), or when a majority of the participants agree to alter the blockchain’s rules.

The distinction between public and private blockchains is less useful with regard to anticompetitive practices using smart contracts. The constraints imposed by blockchain’s architecture apply only to a limited extent in this case, as one can implement them on an upper level. Put differently, the blockchain’s initial characteristics are important to allow smart contracts, but the two levels are not intrinsically linked. It follows that public blockchains can be almost as useful as private blockchains for the implementation of such unilateral practices. Two lessons emerge from this.

First, in terms of the practices directed at the blockchain, I would advise that antitrust agencies focus on behaviors that have the effect of concentrating the blockchain infrastructure by eliminating participants at this layer. Here, agencies should ensure that no anti-competitive practice impacts blockchain development and creates artificial centralization. As blockchain industries mature, this issue will become pressing – the technology will have a more significant impact on the overall economy, serving as one of its underlying foundations.

Second, the sanction of practices using blockchain for anticompetitive purposes (in the “real space”) will help eliminate the artificial centralization of the economy while presenting little risk of indirectly affecting blockchain design. Thus, I advocate for the time being that antitrust agencies focus on these practices (section 2 of the present chapter) rather than on those concerning the blockchain itself (section 1 of the present chapter). Only if and when
blockchains serve as the architecture for the global economy should agencies focus on inside practices.