9. Collusion using blockchain

1 GETTING STARTED

Companies may want to use blockchain to set up collusive agreements concerning the “real space.” While there are clear reasons why companies may want to do so, as opposed to using a non-blockchain medium, it appears even more beneficial for them to augment blockchain with smart contracts. By doing so, they can indeed govern their agreements while benefiting from blockchain’s core characteristics, such as immutability.

1.1 No Smart Contract

Companies may use blockchain to enter into collusive agreements.1 By so doing, their intention might be to ensure the visibility and traceability of any shared information in order to organize their collusion more efficiently. In that respect, public and private blockchains offer distinct advantages.

When the blockchain is public, companies can ensure that they have access to all information listed in the same place, with no user hiding anything from others.2 For example, all the colluders may use a blockchain to share the price of their products. Doing so would reinforce their trust, as it would provide them with a constant flow of immutable information, accessible at all times. That being said, companies may also fear that sharing information on public blockchains will make it easier for enforcers to detect their agreements (though

---

1 See Hitoshi Matsushima, “Blockchain Disables Real-World Governance,” Kyoto University, Institute of Economic Research Working Papers 1017 (2019): 2 (“once a blockchain becomes available, agents can execute agreements regardless of their legality and without help from trusted intermediaries”). Let us note here that setting up a collusion on blockchain does not necessitate in-depth technical knowledge of the technology. Multiple services are offered to companies to help them design a blockchain or use an existing one, see generally “Substrate,” Parity, https://perma.cc/2WMU-2SMG. It can be assumed that blockchain will be used for collusive agreements of a significant size rather than for agreements with little impact on the market.

2 Lin William Cong and Zhiguo He, “Blockchain Disruption and Smart Contracts” (2017): 20 (“greater information distribution may foster collusion which hurts competition”).
the information could be encrypted). It will be interesting to see how this plays out and the extent to which public blockchains will be used to support collusive behavior.

When a blockchain is private, all the companies involved in a collusive agreement get exclusive and secure access to the information. This feature can help strengthen cohesion between them, as it leads to a lower detection risk. Private blockchains also allow the information to be certified before being published, which once again creates a considerable advantage over physical agreements or digital media other than blockchain. And, similarly to public blockchains, the immutability of information published on private blockchains could reinforce the colluders’ trust in each other. For that reason, private blockchains appear to constitute a great medium for organizing collusive practices.

1.2 Smart Contract!

As we have already seen, smart contracts are potential transactions recorded in a blockchain and automatically executed if and when several conditions are met. For example, they can be used for the automatic unlocking of an apartment door rented on Airbnb when the fee is sent to the owner’s account. They can be implemented to create an agreement between companies whose governance follows a combination of smart contracts. But they might also encompass illegal agreements. On top of using a blockchain to collude, companies may set up smart contracts to automate the agreement and make it more predictable and transparent between them.

With a public blockchain, smart contracts can be implemented so that the information published on the blockchain serves as a parameter for the agreement that will be adjusted accordingly. For instance, a smart contract could automate transfers between colluders and make side payments. It could also set a collusive price for sharing markets.

With a private blockchain, smart contracts may serve the same purpose as public blockchains – that is, governing the relationship between users. They may also be used to govern the agreement’s framework by deciding what information is published and who has access to it (which can be changed at any moment in time). Private blockchains allow the most sophisticated level

---


of governance. They would thus be an ideal tool to implement collusive agreements.

Whether they rely on public or private blockchains, smart contracts fundamentally alter the nature of collusion. There are two reasons for this. First, blockchain-based collusion is cooperative. Because these smart contracts are coded directly into the blockchain, their immutability may strengthen collusion’s stability by forcing certain behaviors (as long as they concern online actions, such as making a payment). Second, they make collusion genuinely dynamic. This characteristic is worrying, as one can easily implement smart contracts without technical knowledge.\(^5\)

I will explore these reasons in the next section. For now, let me simply mention that smart contracts may use common libraries and be combined.\(^6\) In other words, the execution of one smart contract could be conditioned to another. This ultimately enables colluders to maintain complex governance mechanisms.\(^7\) In short, they have the potential to make collusion efficient, robust and hard to detect.

2 LIVING UP: THE DOUBLE EFFECT

Cartel stability depends on economic and social elements. Indeed, collusion succeeds when participants have more to gain from cooperation than deviation (the “economic perspective” of cartel stability). Colluders must also trust that none of them will denounce the others by applying for leniency (the “social perspective” of cartel stability).\(^8\) These two perspectives complement one

---


\(^7\) See “Interactions Between Smart Contracts with Solidity,” Zupzup, https://perma.cc/XW9V-F89T (detailing different ways to link smart contracts).

another; indeed, colluders have no interest in leaving the agreement (and
denouncing it) if the illicit gains are high while the risk of detection is low.

Blockchains can be helpful on both fronts. For a start, blockchain provides
colluders with more information than they get using another medium—I call
this the “visibility effect.” At the same time, blockchains also ensure that
agreements are opaque to outsiders, such as non-colluding competitors and
agencies—I call this the “opacity effect.”

2.1 The “Visibility Effect”

Blockchains provide transparency to their participants. Colluders may monitor
each other’s market behavior more easily inside the blockchain than outside
of it. As a result, blockchains prevent the ability to deviate secretly. This
strengthens trust between colluders or, at least, the confidence they have in
the information on which the collusion is based. Blockchains may also correct
deviation by imposing targeted sanctions.

2.1.1 Preventing deviant behaviors

2.1.1.1 More stability

Blockchain may automate governance and therefore prevent deviation. To
understand why this is crucial to colluders, one must first analyze the condi-
tions that make collusion sustainable.

Because anticompetitive agreements are illegal, colluders cannot deploy
legally binding contracts to ensure their implementation. As a result, the
strategy of their co-conspirators is highly unpredictable. They act in their
own interests, making the stability of agreements highly dependent on each
party’s benefits. Thus, collusion is said to be non-cooperative;9 it follows that
the ability to observe each other’s actions and interact frequently is crucial for
stability. “Trust begins where prediction ends.”10

Blockchain helps in that regard. By granting firms access to an extensive
amount of information, public blockchains enhance the ability to observe
other colluders’ practices. The nature of information stays fundamentally the
same. Still, blockchain gathers all information in the same place and ensures
its immutability. This proves helpful to colluders—for example, one company

9 Louis Kaplow, *Competition Policy and Price Fixing* (Princeton University
Press, 2013): 177 (“the fundamental distinction between cooperative and noncoopera-
tive games is that cooperative games allow binding agreements while noncooperative
games do not.”)

10 J. David Lewis and Andrew Weigert, “Trust as a Social Reality,” Social Forces
Collusion using blockchain cannot modify the ledger to hide a deviation from the cartel. Blockchain visibility also prevents deviation because the risk of detection by other colluders is high.\footnote{Margaret C. Levenstein and Valerie Y. Suslow, “What Determines Cartel Success?” Journal of Economic Literature 44, no. 1 (2006): 67, 69.} Of course, the ability to detect cheating is not the only determinant of the cartel’s duration,\footnote{Although it is an important one, see D.K. Osborne, “Cartel Problems,” The American Economic Review 66, no. 5 (1976): 835; see also Nicolas Petit, Droit européen de la concurrence (Lextenso, 2018): 245.} and blockchains will not make cartels indefinite. Still, one may expect collusive agreements to become more stable thanks to the easier identification of deviations.

On top of that, smart contracts may ensure the execution of agreements between participants. For instance, firms could automatically record all transactions and detect unusual transactional flows by any of the colluders, such as a deviation from the collusive price. They could also regulate the price that colluders charge, and smart contracts can allow an automatic distribution of earnings according to pre-defined criteria. Their theoretical immutability is important in that regard;\footnote{See infra Appendix 1.} they have the potential to strengthen the economic and social stability of collusion. Higher (illegal) gains can therefore be achieved.\footnote{See Christopher R. Leslie, “Antitrust Amnesty, Game Theory, and Cartel Stability,” Journal of Corporation Law 31 (2006): 462 (“When players utilizing trusting strategies are paired up, they solve the prisoner’s dilemma in experiments and achieve greater gains than those using distrusting strategies.”); James P. Gahagan and James T. Tedeschi, “Strategy and the Credibility of Promises in the Prisoner’s Dilemma Game,” Journal of Conflict Resolution 12, no. 2 (1968): 224, 226; David M. Messick et al., “Individual Adaptations and Structural Change as Solutions to Social Dilemmas,” Journal of Personality and Social Psychology 44, no. 2 (1983): 294.}

In a sense, smart contracts help to transform collusion into a cooperative game.\footnote{Expressed in terms of game theory, the study of mathematical models for projecting scenarios between players.} The importance of the medium in which the game is played (here blockchain) is often underestimated, yet it is very important in our case. Considering that about half of collusive agreements end because of internal conflicts between their members,\footnote{See Margaret C. Levenstein and Valerie Y. Suslow, “What Determines Cartel Success?” Journal of Economic Literature 44, no. 1 (2006): 43, 75–76.} and that those conflicts mostly arise after deviation by a colluder, one should not underplay the importance of blockchain as a medium.

\footnotesize{
12 Although it is an important one, see D.K. Osborne, “Cartel Problems,” The American Economic Review 66, no. 5 (1976): 835; see also Nicolas Petit, Droit européen de la concurrence (Lextenso, 2018): 245.
13 See infra Appendix 1.
15 Expressed in terms of game theory, the study of mathematical models for projecting scenarios between players.
}
2.1.1.2 Limits

Despite the previous developments, one should not expect blockchain to help the cartelization of the entire economy. Collusion using the technology will, indeed, encounter several limits.

The first relates to the quasi-absence of human intervention in smart contracts’ execution, making them highly inflexible. This creates difficulties for colluders willing to adapt to market fluctuations and other unforeseen events during collusion.\(^\text{17}\) It forces colluders to insert some flexibility into their agreements’ governance by permitting human intervention while trying to maintain blockchain’s immutable features.

Practically, it will require them to design smart “smart contracts” – including narrowly defined clauses for colluders to intervene. Blockchain participants could also use decentralized applications (D-Apps). Any software could be turned into a D-App and be inserted into a smart contract, creating an almost infinite number of possibilities for antitrust and competition law infringements.\(^\text{18}\) The result is that blockchain-based collusion is immutable by nature, which builds trust; but is also adaptable, since D-Apps give colluders flexibility to bring external forces to the very same contract. It allows machines (D-Apps) or physical persons to change the collusion trajectory while maintaining its initial existence. Implementing D-Apps, however, requires technical expertise.

The alternative will be for colluders to encode only part of their agreement on the blockchain and leave the rest to legal contracts.\(^\text{19}\) Such proceedings may prove attractive for parties that wish to avoid smart contracts’ inherent limitations. But in so doing, the parties would lose the assurance that the agreement would be properly executed because it would be (partially) de-automated.

\(^{17}\) Notably, it removes smart contracts from the domain of judicial oversight, including mutual mistake, illegality, capacity, consideration, fraud and duress. See Kevin Werbach, *The Blockchain and the New Architecture of Trust* (MIT Press, 2018): 126.


\(^{19}\) In fact, “[s]everal groups are building solutions using the mutual hashing of smart and legal contracts, including a subgroup of the R3 consortium led by the British bank Barclays, the Monax Burrow software now part of the Hyperledger open source project, and OpenLaw.” See Kevin Werbach, “Trust, But Verify: Why the Blockchain Needs the Law,” Berkeley Technology Law Journal 33 (2018): 489, 544. “Legal contract” is here defined as a “program that runs on the brain of a lawyer,” see Tim Ferriss, “Nick Szabo Interview,” in The Tim Ferriss Show (Podcast), YouTube, published on June 4, 2017, https://perma.cc/Y7Z5-72PY.
They would then engage in the complicated art of maintaining a fair balance between all participants’ interests in the long run.

A second major limit to the stability of collusion using blockchains relates to the use of oracles. When the conditions for triggering smart contracts refer to the information contained within the blockchain, no particular issue of trust arises. For instance, if one designs a smart contract that transfers a token when its value goes over a certain amount, the entire operation can be easily automated. Conversely, when smart contracts refer to information coming from the outside world, an issue appears as to whether one should trust the accuracy of the information documented. For example, if a smart contract is triggered when an aircraft is over an hour late, sending compensation to all passengers, how can one ensure the delay will be properly recorded within the blockchain?

The algorithm or device used to find the information in the real space and document it within the blockchain is called an “oracle.” Oracles are essential to many smart contracts. They reintroduce trust issues because they introduce a single point of failure that can have practical consequences for the stability of the collusion or any type of agreement. For that reason, part of the blockchain community is working toward fixing that issue. Different initiatives are underway; but first, it is important to explain the differences between varieties of oracles, as they each raise specific issues.

Some oracles are physical or tangible devices that measure real-world values, such as temperature or whether a shipment has arrived safely (using chips). Other oracles are intangible and comprise only code. That said, one must make a further distinction between single node oracles and a distributed network of oracles. The first relies on one source of information, while the second combines several oracles to create an average of the information they communicate.

One may logically expect collusive smart contracts to rely mostly on intangible single node oracles. These are highly centralized by nature—which creates a trust issue. Their centralization is also problematic from an antitrust

---


22 As such, they may be used for collusive purposes; on that, see Lin William Cong and Zhiguo He, “Blockchain Disruption and Smart Contracts,” Review of Financial
perspective, as agencies could see the use of the same oracle by several competitors as anticompetitive.23

Several proposals are in development to solve that issue of centralization and reliance. For example, one could use intangible distributed oracles.24 Oracles could also apply a voting game that motivates users to validate the correct data.25 Vitalik Buterin offered one of the first proposals for a trusted data feed by introducing the SchellingCoin.26 Other solutions will be put forward; but for now, oracles are a thorn in the side of colluders.

For that reason, one may wonder whether smart contracts will rely on genies instead of oracles. An oracle is a question-answering machine, while a genie is a command-executing system.27 After receiving a high-level command, the genie seeks to follow the spirit rather than the letter of that command.28 It overcomes the issue of documenting the outside world into the blockchain; the genie works by extrapolating distances to bridge the gap between the two. But of course, genies and other AI-related solutions come with issues in terms of design and subsequent control.

2.1.2 Correcting deviation

Besides preventing deviations, blockchain and smart contracts can be used to punish them. Specifically, the sale of a product at a different price than that agreed upon by colluders could be automatically recorded and punished by smart contracts. These smart contracts could be automated on the basis of several conditions combined (e.g., duration, spread with the collusive price). They would play a part in reinforcing collusion; indeed, the threat of automated and targeted punishments de-incentivizes deviations. After all, “one of the greatest curbs on crime is not the cruelty of punishments, but their infal-
libility … The certainty of punishment, even if moderate, will always make a stronger impression.”

We know from empirical work that intentional deviation must be visibly and effectively punished for collusion to persist. The threat of returning to a competitive situation may deter such behavior, but ideally, the punishment must be directed only at the deviation. Blockchain could help colluders in that regard. One way would be to request an initial payment of tokens to participate in the agreement and then automatically regulate their distribution based on the party’s compliance. But of course, this would require a rather large monetary sum that could be picked up during annual audits. More simply, one could adjust the blockchain’s participation fees according to each colluder’s past behaviors or expectations, making it more expensive for certain members to be part of, or deviate from, the agreement.

Unintentional deviation is usually not as problematic for the cartel’s stability, as long as it does not occur too often and deviations are compensated in a way that preserves each colluder’s interests. Blockchain and smart contracts make that possible, as they can be used to ensure a fair balance by redistributing any extra profits made by a deviation between all colluders. Here again, they improve the stability of collusive agreements.

Whether the deviation is intentional or not, smart contracts should indeed compensate for the gains made by a deviating member to avoid the possibility of lucrative infringement (which occurs when the benefits are higher than the punishment). This economic element of cartel stability depends on the perceived and actual profits that result from cheating compared with the likelihood of punishment by other colluders. By increasing the detection of

deviation and the potential accuracy of sentences, blockchain will raise the costs of misbehaving and make collusive agreements more stable.

2.2 The “Opacity Effect”

Despite creating a strong “visibility effect,” blockchain generates a concomitant “opacity effect;” it does not make information available to everyone – and especially not to competitors and agencies. Blockchain increases members’ trust in one another because it protects them from being detected, which has great implications for agencies’ investigations.

2.2.1 Detection

2.2.1.1 Stability

As I have shown, public and private blockchains provide users with different opacity settings. Public blockchains are freely accessible, and all the information they contain is part of the public domain. Anyone can access it without even “entering” the blockchain.35 One needs no membership or authorization. For example, the history of all Bitcoin transactions is open to all, regardless of whether one is a Bitcoin owner. Private blockchains have opposite features. Information stored on private blockchains is available only to its users and can be channeled to just some of them.36 Both types of blockchain, however, generate a “visibility effect” (among colluders) while producing an “opacity effect” (among non-colluders).

This double effect exists on public blockchains because all transactions are hashed through cryptographic functions,37 and because users’ identities are protected by pseudonymity. For instance, only the sending and receiving punishments, which are costly.”). More generally, see Richard J. Gilbert, Innovation Matters: Competition Policy for the High-Technology Economy (MIT Press, 2020): 117.


36 See Kevin Werbach, The Blockchain and the New Architecture of Trust (MIT Press, 2018): 96 (“[Private blockchain] generally provide[s] granular controls on who can see and manage information on the ledger … A permissioned distributed ledger system grants control over access. It may also grant parties different levels of visibility into transactions compared to the fully transparent approach of public blockchain systems.”)

37 See id. at 45 (“Converting a file into a hash is easy but going from the hash back to the original file is virtually impossible except through massive trial and error.”) Generally speaking, hashing is the process of taking an input (information on the blockchain) and turning it into a cryptographic output.
Bitcoin addresses, the Bitcoin amount and a timestamp appear on the Bitcoin blockchain. On Ethereum, one may identify whether the transaction results from a smart contract (as this information shows), but the agreement’s terms remain secret. More specifically, the source code of the smart contract itself (e.g., the Solidity code for Ethereum’s smart contracts) is generally not stored on the blockchain. Only the compiled bytecode is stored on it, so that the Virtual Machine can execute the smart contract when it is being called. One cannot convert that bytecode back into the original programming language without missing information. A meticulous translation could give a sense of what the smart contract is all about, but that is about it.

As a result, analyzing the transactions made by one user can prove useful for discerning a pattern, but the transaction’s exact nature remains mostly secret. The opacity effect is even more substantial with private blockchains because their existence may be kept secret, and their entry subject to specific conditions and approval.

Blockchain thus protects colluders from detection by antitrust and competition authorities. As I discussed in Chapter 2, the protection is not foolproof, but is definitely greater than that which exists outside of blockchain ecosystems. And when the fear of exposure is partially or entirely dispelled, it reinforces the mutual trust that colluders have.

---

39 See, for instance, Etherscan, https://etherscan.io/tx/0x9bd7d73bce1c3a420093c7f82e150874136968df1ca418f23e4e3a8f4 (indicating “Contract 0xda4c48e0b24039969fcf16d1cd6262eab821d3384 Gitcoin Grants: Tornado.Cash”).
40 Yi Zhou, Deepak Kumar, Surya Bakshi, Joshua Mason, Andrew Miller and Michael Bailey, “Erays: Reverse Engineering Ethereum’s Opaque Smart Contracts,” in 27th Security Symposium 18 (2018) (showing that 77.3 percent of smart contracts have not released public source codes and remain opaque even after using a decompiler). For a counter-example, see Ethereum (ETH) Blockchain Explorer, Etherscan https://etherscan.io/address/0xeb17adcc8cf24d2d6813f50f647b613df01014a2#code.
This shield provided by blockchain is critical in terms of collusion longevity, as “a rise in the probability of detection and conviction causes the immediate collapse of the least stable cartels.” Antitrust agencies seek to create a prisoner’s dilemma in which each player shares the same dominant strategy: to report the agreement. This outcome can be achieved only if one can detect the collusion. Because of blockchain’s protection, it becomes harder for antitrust agencies to create an incentive to deviate – the overall level of stability increases. To be sure, detection by antitrust agencies is not the only way collusion can end. On top of the economic returns from deviation, or the collusion simply losing its financial value (because of changes in the market), leniency procedures and complaints from outside the agreement are two significant causes. Nevertheless, empirical studies show that collusive agreements have a shorter duration when antitrust authorities expand enforcement efforts toward detecting them.

2.2.1.2 Type

On top of affecting cartel stability, the opacity effect will affect the types of agreements that colluders agree upon. The increase in trust thanks to blockchain will lead to more aggressive collusion. If the detection risk is high, colluders should, in their best interests, set up an agreement that deviates only slightly from the competitive price. But where the detection risk is low, colluders should deviate substantially from the competitive price. Anticartel enforcement influences firms’ behavior, and when it disappears, one can expect behaviors to change.

In a nutshell, blockchain helps cartel stability because of the double effect, and it also changes the nature of the agreement. I remain curious to see whether companies will massively use blockchain to set up illegal agreements. For one thing, blockchain is often presented as a “big open book,” immutable by nature. Companies may fear using it for that reason, despite the opacity effect. They may also be wary of using blockchain for such a purpose because immutability does not allow for much flexibility. That, however, remains to be seen.

45 Although a high collusive price could also raise each firm’s individual incentive to deviate.
Human’s tendency to be overconfident—that “everything will go according to the plan”\textsuperscript{47}—remains a strong driver of behavior. Companies could (will?) very well use blockchain precisely because it is immutable and allows them to enforce their original intentions. I leave this analysis to behavioralists.

2.2.2 Agencies’ investigations

The opacity effect does not entirely prevent antitrust agencies from detecting collusion. Two methods can be used to identify such agreements: one reactive, the other proactive (\textit{ex officio}).\textsuperscript{48}

The reactive method mainly consists of using complaints, whistleblowers, grand juries, informants, search warrants, dawn raids and leniency applicants, which blockchain cannot prevent.\textsuperscript{49} Still, by reinforcing trust between colluders (social perspective), this method might prove less efficient in the coming years than it is today. I study why that is in the following pages. But for now, the focus on agency investigations leads me to consider the proactive method, which translates into market surveillance, industry monitoring and screening. It is the method that is the most affected by the “opacity effect.”

Proactive methods aim to identify anticompetitive effects visible outside of the blockchain. There are two sub-types of approaches to the proactive detection of collusive agreements: one structural and the other behavioral.\textsuperscript{50} The structural approach involves screening specific markets to identify collusive agreements. Typically, an antitrust authority decides on the industry to screen and determines whether it exhibits characteristics that make the firms inclined to collude. The behavioral approach flags firms’ behaviors or market outcomes to detect any patterns of collusive agreements.\textsuperscript{51} Both types eventually rely on market-based evidence from pricing patterns.\textsuperscript{52}


\textsuperscript{50} Id. at 20.


\textsuperscript{52} See Louis Kaplow, \textit{Competition Policy and Price Fixing} (Princeton University Press, 2013): 259 (“Certain pricing patterns may indicate successful oligopolistic coordination or a breakdown that implies its prior existence.”) For a list of these patterns, see OECD, “Ex Officio Cartel Investigations and the Use of Screens to Detect Cartels,” DAF/COMP(2013)27 (2013):28.
Considering that, in the words of Richard Posner, “[e]conomically signif-
icant collusion should leave some visible traces,” blockchain does not nec-
essarily help companies when it comes to these proactive methods. Collusion
impacting prices to end consumers will remain visible to everyone’s eyes;
here, the medium is not relevant. Things are different for collusion regarding
business-to-business prices (between companies in the production chain).
These prices are often not publicly available, and blockchain will complicate
the investigation of antitrust agencies by encrypting most of the relevant infor-
mation. Only a more collaborative “law + technology” approach may avert this
outcome, as I will explore in Part 3.

3 EVERYTHING COMES TO AN END

While blockchain is conducive to collusive agreements, it can also precipitate
their downfall when smart contracts automate the exit from collusion. In the
end, blockchain strengthens the cohesion of colluders, and it speeds up collu-
sion unfolding after the first dissension appears. One should therefore expect
the number of leniency applications to decrease as they typically result from
ailing cartels.

3.1 Smart Ending

Smart contracts may be used to exit collusive agreements, whether to force the
exclusion of a colluder deviating from the cartel or for a company to manage
its own exit. One might organize these automated exits following several
pre-established rules, ultimately leading to extra challenges for antitrust
agencies.

3.1.1 Forcing exclusion

Smart contracts are useful to prevent co-conspirators from deviating. As soon
as a conspirator is caught selling its products below the agreed price, she or he
can be automatically ejected from the agreement. If all the colluders know this
mechanism, it will strengthen their incentive to comply.

In practical terms, none of the colluders has the power to exclude each other
from a public blockchain. Smart contracts’ governance could, however, organ-
ize exclusion from the agreement running on top of such a blockchain. As far
as private blockchains are concerned, the exclusion may be total or partial.
Colluders deviating from the cartel could be excluded entirely from the block-

chain or only from certain functions, such as adding or validating information and reading part of the blockchain.

Finally, empirical evidence suggests that the stability of collusion is endangered after sanctions are imposed against deviations.\(^5^4\) That is why colluders generally invest in detection tools, which help prevent deviation and maintain the agreement.\(^5^5\) Colluders will then be required to set these sanctions at an appropriate level. On the one hand, implementing smart contracts makes it possible to dissuade deviant behaviors and manage collusive agreements. On the other hand, punishments should not be too strict or too frequent. In short, despite the help of blockchain, running collusive agreements remains a complex endeavor.

3.1.2 Exiting

Parties can also use smart contracts to exit collusive agreements, whether this is automatic (as soon as one identifies specific deviant behaviors) or on-demand. Theoretically, smart contracts will speed up the dissolution of collusive agreements when they start to falter. Such a situation occurs when colluders suspect that an antitrust agency may detect the collusion (causing “death by antitrust”), or when there is a strong disagreement between colluders (leading to a “natural death,” which the blockchain alone cannot prevent). By facilitating the identification of deviation, blockchain is a means of speeding up its dissolution when it turns sour.

Nonetheless, one may question whether companies will use smart contracts to exit an illegal agreement while leaving evidence of the collusion behind or if they will first try to hide their past behaviors. Of course, users’ identities are protected by pseudonymity,\(^5^6\) and most information regarding their transactions is encrypted. But colluders can do more – namely, use different technics


\(^{5^5}\) J.D. Jaspers, “Managing Cartels: How Cartel Participants Create Stability in the Absence of Law,” European Journal on Criminal Policy and Research 23, (2017): 319, 322 (“[C]artels invest more in means to prevent cheating than to resort to ex post punishments, which are costly.”)

\(^{5^6}\) See Kevin Werbach, The Blockchain and the New Architecture of Trust (MIT Press, 2018): 179 (“The supposed anonymity of the blockchain is also not an absolute bar against legal enforcement. Firms such as Elliptic and Chainalysis work with law enforcement agencies to track down criminals by analyzing cryptocurrency transaction patterns.”) There is a (never-ending?) race. It remains uncertain which of the developers or tracking companies will win it – if either one ever does. Ethereum, which is working on incorporating quantum resistance into its design, shows that the barriers created by blockchain are getting higher.
to overcome immutability. A first set of solutions consists of bypassing immutability, thereby creating a technical workaround without impacting it. For example, colluders could simply store the hash of the data on the blockchain while storing the actual data elsewhere. Alternatively, they could delete the encryption key before leaving the blockchain. As previously explained, this will prevent the retrieval of the data.

A second set of solutions consists of impacting immutability. This could be done using a chameleon hash function. Here, trusted users (e.g., the colluders) access a trapdoor key to change the information while maintaining chain integrity. Alternatively, colluders could use mutable blockchains recording various possible versions of transactions or flexible memory blockchains that enable changes while preserving the integrity of hash values. Should they want to change the version of their transactions before exiting the blockchain, they could then use meta-transactions. Another solution consists of using

---


a data structure that allows blockchain users to retract information without changing the hash value of recorded blocks.62

Of course, these solutions are technical and would have to be implemented from the moment the collusion is created. Colluders will not do so in most cases. But either way, establishing the link between the data found on the blockchain and the collusive practices will remain a challenge for agencies.63 That said, fears are (sometimes) irrational, and companies may still be reluctant to collude on a public permissionless blockchain.

The same goes for private blockchains although it is well known that the owner may have the right to override, edit and delete information.64 The colluders will thus have to convince her or him (the owner) to remove the incriminating information before they terminate their agreement. If all colluders agree to delete the information, this will be easier to perform than if they were using a public blockchain. And because it is easier to obtain a voting majority on small private blockchains—where all the participants may be colluders—than on large and public ones, private blockchains appear to be a better medium for colluders.

3.2 Leniency 2.0

Blockchain, coupled with smart contracts, may cause a decrease in the number of leniency applications. This is not necessarily as problematic as it seems, considering that smart contracts can also put an end to illegal practices.

3.2.1 Blockchain and leniency

Studying the impact of blockchain on leniency applications requires consideration of three elements.

---

63 Dawn raids are unannounced inspections conducted by antitrust agencies at companies’ premises with the goal of finding incriminating evidence.
The first relates to the current trends in leniency applications in both Europe and the United States. Introduced in 1978 by the DOJ\textsuperscript{65} and in 1996 by the European Commission,\textsuperscript{66} the leniency procedure enables colluders to self-report their illegal behavior and hand over evidence in exchange for (partial) immunity from legal sanctions. It is critical to ensure the detection, investigation and prosecution of hard-core cartels and other types of collusion. Over the years, leniency has become the “most effective tool in the fight against cartels.”\textsuperscript{67} The DOJ also stated that: “The Program (and its counterpart for individual leniency applicants) has been an incredible success in deterring and detecting antitrust crimes.”\textsuperscript{68} It is the “most important investigative tool for detecting cartel activity.”\textsuperscript{69}

Still, several studies estimate the annual probability that a cartel would be detected, conditional on being detected, at 13–17 percent.\textsuperscript{70} This low detection rate proves that leniency procedures are not sufficient in and of themselves. On top of that, the number of leniency applications fell by half in Europe between 2014 and 2016.\textsuperscript{71} One can observe the same trend in the United States.\textsuperscript{72} This shows that the leniency procedure faces important challenges. Blockchain will not make things any easier.


\textsuperscript{66} Id. at 10 (“In 1996, the European Commission (EC) adopted its first Leniency Notice.”)

\textsuperscript{67} Id. at 18. In Europe, “leniency policy covers purely administrative liability of companies and does not extend to individuals.” Id. at 29. This is different in the United States. According to the European Commission, “the leniency policy proves very successful,” see “Cartels: Leniency,” European Commission: Competition, https://perma.cc/ZM33-KWUF.

\textsuperscript{68} “Silver Anniversary: The Antitrust Division’s Leniency Program Turns 25,” U.S. Department of Justice, April 10, 2018, https://perma.cc/9Q8B-QVBB.


\textsuperscript{71} See Johan Ysewyn and Siobhan Kahmann, “The Decline and Fall of the Leniency Programme in Europe,” Concurrences Review, 1-2018 (2018): 44, 45 (“In 2014 there were 46 leniency applications, which dropped to 32 applications in 2015, and finally only 24 applications have been registered in 2016.”)

The second element concerns the technical difficulties created by blockchain, as it will complexify the work of antitrust agencies. First, blockchain protects users’ identities. That is all the more so with public blockchains, where there is no need for the creator of a blockchain to approve users. Second, the transactions recorded on the blockchain are encoded and cannot be decrypted by anyone other than the parties to a transaction. This encryption also protects colluders by preventing agencies from tracing the history of their collusion. Third, even if users’ identity and purpose of their transactions were known, the deletion of the data contained therein by agencies would remain quite challenging (to say the least). In this respect, perhaps the exit of companies with the automatic destruction of information by smart contracts would be preferable to a leniency application with no subsequent possibility of eliminating the collusive agreement, or at least, the information illegally published.

The third element is linked to the fact that, besides its technical characteristics, blockchain enables colluders to manage the risk of detection. In turn, this should reduce the number of leniency applications. Most of these procedures are indeed started by colluders who fear being discovered. Technology helps in that regard. This is all the more true with private blockchains, as they can be set up so that only specific users can access the entire blockchain. This will limit their ability to hand over incriminating information to antitrust agencies. As a result, when choosing between leniency and an exit through smart contract, there is every reason to believe that blockchain would, at least partially, overshadow leniency applications.

How worrying is all this? At first sight, the expected decrease in the number of leniency applications may seem problematic, as antitrust agencies rely heavily on them to detect collusive agreements. According to the Organisation for Economic Co-operation and Development (OECD), the percentage of cartel cases detected through leniency applications is reported in the survey to range between 45 and 55 percent for countries such as Canada, Chile, Germany, Korea and New Zealand, and over 85 percent for the European Union.

73 Once again, immutability can be undermined only with the approval of a majority of blockchain users, unless proper mechanisms have been implemented from the start.
75 Id. at 22; see OECD, “Ex Officio Cartel Investigations and the Use of Screens to Detect Cartels,” DAF/COMP(2013)27 (2013): 9, 108 (noting that “in some jurisdictions leniency programme cases have ‘crowded out’ efforts to expose cartels by other means,” but also stating that although competition authorities tend to deny it, “[i]n the recent past the majority of the Commission’s cartel cases have originated from leniency. At the same time, the Commission has continued pursuing cases also on ex officio basis.”)
Union.\textsuperscript{76} In the United States, more than 90 percent of the penalties imposed by the DOJ in recent years are linked to investigations assisted by leniency applicants.\textsuperscript{77} This report shows a reactive policy by antitrust agencies. It also signals to companies that a well-designed collusive agreement that frames and rectifies disagreements has a good chance of (extended) survival.\textsuperscript{78}

By undermining leniency programs’ effectiveness, blockchain will force competition agencies to become proactive again, failing which companies will have a growing sense of impunity from antitrust and competition law. Only a strengthening of proactive detection will increase the risk of punishment and force companies to seek leniency again.\textsuperscript{79}

### 3.2.2 A (almost) similar end

In its Notice on Immunity from fines and the reduction of fines in cartel cases, the European Commission argues that leniency programs exist to detect and end illegal collusive agreements.\textsuperscript{80} The European Commission stresses that “by their very nature, secret collusive agreements are often difficult to detect and investigate,” and that rewarding undertakings that are willing to put an end to their participation is in the community’s best interest.\textsuperscript{81} The United States shares a similar view, where leniency programs are seen as a “prompt and effective” means to stop companies from further participation in collusive agreements.\textsuperscript{82}


\textsuperscript{79} See \textit{id.} at 5.

\textsuperscript{80} In theory, the leniency application is open only to horizontal cartels and leaves out the exchange of information. European Commission, “Commission Notice on Immunity from Fines and Reduction of Fines in Cartel Cases, O.J. 2006/C 298/11,” Official Journal of the European Union (2006).

\textsuperscript{81} \textit{Id.} at 17.

Smart contracts can achieve the same end. By discouraging firms from cheating on cartels, by automating punishments and by giving a means to exit the agreement under predetermined conditions, one may expect that the number of leniency applications will drop. But this decrease is not necessarily as problematic as it seems.

I have explained that an increase in the number of “natural” deaths is expected thanks to smart contracts. This tendency to move away from self-reporting and toward the self-regulation of collusive agreements operating on blockchain could eventually manifest itself in two ways: by making collusive agreements robust during their existence with very few deviant behaviors, and by making their disappearance sudden. Put differently, one can expect an increase in the number of collusive agreements along with an increase in their profitability, but not necessarily in their duration.

Therefore, the partial demise of leniency proceedings should not be a significant concern for stopping illegal behavior. In fact, one could point out that blockchain will lead to a faster dissolution of collusive agreements than leniency programs currently do. Studies suggest that leniency helps detect unprofitable and poorly designed collusive agreements; in short, those that are about to collapse anyway. Blockchain will do the same, but potentially more rapidly.

But of course, there is a difference between ending collusion thanks to smart contracts or leniency – an important one. Without public sanctions being imposed by an antitrust agency, private enforcement will be hindered. This will deter affected parties from recouping the damages they have suffered. It follows that smart contracts will impact the chain that enables damages to be compensated – especially in Europe, where private enforcement follows public enforcement more commonly than in the United States.

4  CHAPTER SUMMARY AND BEYOND

In this chapter, I have explained that blockchain is the rainforest of tomorrow’s collusive agreements: full of original life forms and alternative possibilities. Blockchain gives rise to unidentified creatures and dangerous species. This is all the more true if companies use smart contracts to increase collusive

---

83 Indeed, if “the possibility for a deviator to apply for leniency increases the payoff of cheating, thus making collusion more difficult to sustain,” quite the contrary is also true. See Wouter P.J. Wils, “Leniency in Antitrust Enforcement: Theory and Practice,” World Competition Law & Economic Review 30, no. 1 (2007): 25.

84 On the contrary, European follow-on enforcement, which requires first a decision coming from a public agency to introduce a subsequent trial, will likely disappear in such scenarios without being replaced by any blockchain mechanism.
agreements’ stability. Illegal practices then become visible to colluders while ensuring their opacity to non-colluders. As a result, collusion becomes more robust because deviation is easier to detect, but it (perhaps paradoxically) ends more abruptly. One could sum up these findings as outlined in Table 9.1

Collusive agreements using blockchain will significantly affect the real space. First, they will increase artificial centralization by increasing colluders’ ability to go unchallenged. Second, they will constrain non-colluding companies facing such cartels. For these reasons, antitrust law enforcement must become proactive in eliminating collusions and re-establishing decentralization. Otherwise, participants will not be able to compete under a classic Darwinian process. So, here again, the law could be the ally of blockchain communities. I will discuss how this could happen in Part 3; but before I do, I want to explore monopolization and abuses of dominant positions, as blockchains may also lead to this type of behaviors.

Table 9.1  Smart contracts in the context of collusion

<table>
<thead>
<tr>
<th>Type of smart contract</th>
<th>At the creation of collusive agreements</th>
<th>During the life of collusive agreements</th>
<th>Causing the death of collusive agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>What: smart contracts ensuring the efficiency of traditional collusion (i.e., whose effects are manifested outside of the blockchain)</td>
<td>What: smart contracts preventing deviant behaviors Objective: to ensure trust between colluders by automating transactions and publishing trustworthy information</td>
<td>What: smart contracts forcing one deviant colluder to exit the blockchain Objective: to eject a deviant colluder (when the deviation cannot be forgiven) to recreate a trustful environment</td>
</tr>
<tr>
<td></td>
<td>Objective: collusion using the blockchain as a trustful medium and smart contract as a governance tool</td>
<td>What: smart contracts correcting deviant behaviors Objective: to impose targeted punishments as compensation for the deviation and to recreate trust between colluders</td>
<td>What: smart contracts allowing one colluder to exit the blockchain at will Objective: to create trust between colluders by providing them an exit gate (prevent entrapment)</td>
</tr>
</tbody>
</table>