Harvard Journal of Law & Technology
Volume 33, Number 1 Fall 2019

COLLUSION BY BLOCKCHAIN AND SMART CONTRACTS

Dr. Thibault Schrepel[*]

TABLE OF CONTENTS

[*] Assistant Professor at Utrecht University School of Law, Faculty Associate at Harvard University's Berkman Klein Center for Internet & Society, Associate Researcher at University of Paris 1 Panthéon-Sorbonne, Invited Professor at Sciences Po Paris. Thanks to Maurits de Munck for his research assistance and to Mark Lemley, Frédéric Marty, Viktorija Morozovaite, Margot Daly, Spencer Waller, Kevin Werbach, Paul de Bijl, Nathan Kaiser as well as workshops participants at OECD Global Blockchain Policy Forum 2019, Utrecht University's RENFORCE Center, Stockholm University, University of Groningen, EFTA and AGCOM for their comments and feedback. The author also expresses his gratitude to JOLT's editors for their excellent assistance during the editing process. No outside funding was received or relied upon for this paper. I do not have any financial interest at stake in blockchain.

> ONE OF THE GREATEST CHECKS ON CRIME IS NOT THE CRUELTY OF PUNISHMENTS, BUT THEIR INEVITABILITY. . . . THE CERTAINTY OF A CHASTISEMENT, EVEN IF IT BE MODERATE, WILL ALWAYS MAKE A GREATER IMPRESSION THAN THE FEAR OF A MORE TERRIBLE PUNISHMENT THAT IS UNITED WITH THE HOPE OF IMPUNITY . . . .
>
> — CESARE BECCARIA[1]

I. INTRODUCTION

Blockchain may transform transactions the same way the Internet altered the dissemination and nature of information.[2] If that were to be the case, all relationships between companies would change, including prohibited ones. For that reason, the stakes are crucial[3] and the absence of academic studies entirely dedicated to this issue must be remedied. These studies must be completed without further delay, as the ever-

[1] CESARE BECCARIA, ON CRIMES AND PUNISHMENTS 46 (David Young trans., Hackett Publishing Co. 1986) (1764).

[2] For an understanding of how innovation is spreading, see EVERETT M. ROGERS, DIFFUSION OF INNOVATIONS (Free Press 5th ed. 2003) (1962). Some argue that citizens will use the blockchain in some capacity in the near future, whether it is to vote, to buy food, or to implement any kind of transactions. *See, e.g.*, Emmanuelle Ganne, *Can Blockchain Revolutionize International Trade?*, WORLD TRADE ORG. (2018), https://www.wto.org/english/res_e/booksp_e/blockchainrev18_e.pdf [https://perma.cc/HYG3-Y26T].

[3] On whether cyberspace (the Internet) required new regulations, see Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996). For a positive answer, see Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 675–76 (1998).

evolving nature of technology complicates the application of law to blockchain.

It is therefore essential that antitrust and competition laws stay up-to-date because these laws play a great role in shaping the power that flows from technologies and the way companies interact with each other. This Article aims to contribute to antitrust and competition law modernization by focusing on the interplay between blockchain and collusive agreements.

A. The Technology: Blockchain Toolbox

In this Article, I first intend to explain how the blockchain technology works and to describe its main characteristics. Although knowing how to code a new blockchain could be useful in better understanding the legal implications it creates, I believe that it is not an absolute necessity. The same is true for all scholarship studying the impact of the Internet: the most important thing is to understand what the technology can do.

A blockchain is an open and distributed ledger recording all sorts of transactions between users. With a blockchain, the ledger is maintained across the computers of all blockchain users through a peer-to-peer network. As a result, a blockchain can do virtually everything that a computer does, but with four characteristics that differentiate it.[4]

First, blockchain is decentralized. This is because blockchains are distributed ledger systems, meaning that no single user controls the information or the data on the blockchain, and that no one is in charge of maintaining its proper functioning. More specifically, public blockchains have no proper governance outside of the consensus mechanism.[5] Its creators do not control who accesses, uses, and exits the

[4] *See generally* RACHEL BOTSMAN, WHO CAN YOU TRUST?: HOW TECHNOLOGY BROUGHT US TOGETHER AND WHY IT MIGHT DRIVE US APART (2017); Stefan Kulk, *Blockchain 101*, UTRECHT UNIVERSITY, https://blockchain.regulatingbig.tech [https://perma.cc/KU72-NWWN] (providing a video explanation of the distributed nature of blockchain).

[5] At least not yet. There are initiatives to create true on-chain governance. *See* KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST 217 (2018) ("A project called Rootstock is trying to create a smart-contract layer on top of Bitcoin. It incorporates a built-in process giving both miners and users the power to make binding votes on network changes. Projects such as Decred, Dfinity, and Tezos are building entirely new blockchains with governance mechanisms baked in. These systems use algorithms to allow network participants to vote on changes to the protocol."). Here is a paradox. Blockchain provides its users with true decentralization, and yet, decentralization at a big scale often calls for governance. On the subject of rejecting governance on the Internet (and therefore on blockchain), see Paulina Borsook, *How Anarchy Works*, WIRED (Oct. 1, 1995, 12:00 PM), https://www.wired.com/1995/10/ietf [https://perma.cc/27SX-WGTH] (noting that the Internet Engineering Task Force ("IETF") mantra is "We reject: kings, presidents, and voting. We believe in: rough consensus and running code."). *See also* GEORGE GILDER, LIFE AFTER GOOGLE: THE FALL OF BIG DATA AND THE RISE OF THE BLOCKCHAIN ECONOMY 257–67 (2018).

blockchain.[6] Because there is no central point of failure, blockchains are said to be secure and reliable by nature.[7] Additionally, blockchains function on peer-to-peer transmission, which also contributes to making blockchain a decentralized technology. All information exchanged on blockchains is conveyed between each user — in technical terms, between each node (a computer connected to the network).[8]

Second, blockchain relies on unstoppable code.[9] The first key feature in this respect is the consensus mechanism, which is the general agreement under which the blockchain operates. As of today, the most commonly used consensus mechanisms are Proof of Work, Proof of Stake, Proof of Burn, Proof of Authority, Proof of Capacity, and Proof of Storage, but new ones are being introduced frequently. Depending on which consensus mechanism is chosen, users will make different uses of computational logic on blockchain. All transactions happening on blockchain may be programmed and automated by smart contracts,[10] defined as "a computerized transaction protocol that executes the terms of a contract,"[11] or in other words, "a program enforce[ing] the contract built into the code."[12] When users set up such algorithms that automatically trigger transactions between nodes, the transactions are validated according to the chosen consensus mechanism.

Third, blockchains are pseudonymous. Each node has a unique alphanumeric address, called the public key, which consists of a specified number of characters.[13] This key is derived from a private key that each

[6] By default, it is impossible to "exit" a public blockchain because there is no need to "enter" it in the first place; its access is universal. Bitcoin is a good example of a public blockchain, since anyone can buy or sell the quantity of the currency that they want. The crypto-currency is not controlled by anyone in particular, but instead by all its users together.

[7] In fact, the more mining there is, the more the blockchain is secured because the additional mining reduces the likelihood of a 51% attack. On blockchain eliminating different points of vulnerability on the Internet, see GILDER, *supra* note 5, at 171.

[8] *See* Maryanne Murray, *Blockchain Explained*, REUTERS (June 15, 2018), http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html [https://perma.cc/ZA8U-QN3S]. A blockchain consists of a network of computers, so-called "nodes," which check the details of the transactions to make sure they are valid. A central node holds authority in centralized networks, while all nodes access all information and compete on an equal level in decentralized networks.

[9] Rhys Lindmark, *#CryptoEthics Concepts: Decentralization-Enabled Unstoppable Code*, GREY MIRROR (July 8, 2018), https://www.rhyslindmark.com/cryptoethics-concepts-decentralization-enabled-unstoppable-code [https://perma.cc/VNR2-94KM].

[10] *See infra* Appendix 1: Trust by Smart Contracts Through the Existence of Collusion.

[11] Nick Szabo, *Smart Contracts*, UNIVERSITEIT VAN AMSTERDAM (1994), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html [https://perma.cc/5NF3-R6N3].

[12] H.R. REP. NO. 115-596, at 210 (2018).

[13] This is true for all public blockchains and some types of private blockchains. Private blockchains may also give a limited membership without pseudonymity. *See* JONES DAY, BLOCKCHAINS AND ANTITRUST: NEW TECHNOLOGY, SAME OLD RISKS? 1–2 (Aug. 2018), https://www.jonesday.com/files/Publication/92640617-6a6a-45b4-8f82-18d5e65d5b40/Presentation/PublicationAttachment/c9c5c7fa-4f65-4758-b00f-1a970848eb13/Blockchains_

user stores outside the network. As a consequence, this private key cannot be seized, which protects users' identities. Even if the private key is given away by one user, it does not reveal its "real life" identity.[14] Moreover, blockchains can also be used to hide the meaning of transactions: only the exchange of tokens is made public, not the reason why they were exchanged in the first place. The same is true for cash, but not for credit and debit card payments, in which banks know the identities of the transacting parties. In short, "nobody knows you're a dog"[15] on a blockchain, and this is all the more true if colluders combine their blockchains with other mechanisms to further protect their identities and the content of their transactions. Such mechanisms can be "off-chain" or "sidechain."[16] "Off-chain" mechanisms are used to store confidential information separately on another system with access control restrictions. They can be useful for colluders in restricting access to transaction details to authorized parties only. "Sidechains" are parallel blockchains working alongside the primary blockchain. They will complicate the work of antitrust and competition agencies in analyzing potential anti-competitive behaviors.

Fourth and last, blockchains are immutable. This is reflected by the fact that records cannot be easily modified along the way.[17] All transactions on blockchain typically reference previous transaction outputs as well as new transaction inputs.[18] Transactions are submitted to the

and_Antitrust.pdf [https://perma.cc/S6GH-ERPY]. Indeed, "[t]his is because the establishment of one's identity is required to participate as a member of the permissioned blockchain network." DYLAN YAGA ET AL., NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, NISTIR 8202, BLOCKCHAIN TECHNOLOGY OVERVIEW 5 (Oct. 2018).

[14] Zero-knowledge proof is a concept in cryptography that provides many interesting applications to blockchain. A zero-knowledge proof exists where a prover A can prove that he knows information X to a verifier B without communicating any information to B other than the fact that A knows X. Thus, prover A does not have to share details, such as the sender's or recipient's identity, with verifier B. Consequently, zero-knowledge proof enforces anonymity in transactions. *See* Brian Curran, *What Are Zero-Knowledge Proofs? Complete Beginner's Guide*, BLOCKONOMI (Oct. 11, 2018), https://blockonomi.com/zero-knowledge-proofs [https://perma.cc/LQN2-4KVM].

[15] *See* Michael Cavna, *'NOBODY KNOWS YOU'RE A DOG': As Iconic Internet Cartoon Turns 20, Creator Peter Steiner Knows the Joke Rings as Relevant as Ever*, WASH. POST (July 31, 2013), https://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb_blog.html [https://perma.cc/6JU4-EPCQ].

[16] WINSTON MAXWELL & JOHN SALMON, HOGAN LOVELLS, A GUIDE TO BLOCKCHAIN AND DATA PROTECTION 16 (Sept. 2017), https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf [https://perma.cc/3HPZ-VBJY].

[17] Unless a fork is created. This is true for the actual data. On the contrary, "applications using the blockchain as a data layer work around this by treating later blocks and transactions as updates or modifications to earlier blocks and transactions. This software abstraction allows for modifications to working data, while providing a full history of changes." YAGA ET AL., *supra* note 13, at 46.

[18] Brad Finney, *Blockchain and Antitrust: New Tech Meets Old Regs*, 19 TRANSACTIONS 709, 712–13 (2018) (discussing blockchain's ledger-like characteristic).

blockchain, and once they are buried under enough confirmations that the contained information is accurate, they become irreversible[19] and can in principle be seen by all users with no restriction to access. Without the guarantee of immutability, blockchain is nothing more than a service similar to on-demand cloud computing platforms such as Amazon Web Services ("AWS"), "which is already much more user friendly and a thousand times cheaper."[20] Precisely because blockchain is immutable, different mechanisms, called consensus mechanisms, may be used to sort out which information and transactions are recorded on the blockchain.[21] This creates trust, as everything on a blockchain has been verified at some point in time.[22]

These different characteristics of blockchain lead to different uses of the technology.[23] The first (blockchain 1.0) is crypto-currency, in which blockchain tokens are traded outside of the sole blockchain system.[24] The second (blockchain 2.0) is smart contracts, in which blockchain is used to implement automated transactions between users by executing pre-defined algorithms.[25] The third (blockchain 3.0) encompasses all other uses of blockchain, including peer-to-peer ridesharing,

[19] "Each block is recorded using an algorithm that encoded every prior block in the blockchain. Thus, once a block is added to the chain, it is virtually impossible to modify. Any change would require modifying every subsequent block of data on the chain." JONES DAY, *supra* note 13, at 1.

[20] Omar Faridi, *Blockchains Must 'Guarantee Immutability' to Remain Competitive, Ethereum Classic Developer Says*, CRYPTOGLOBE (Oct. 11, 2018), https://www.cryptoglobe.com/latest/2018/10/blockchains-must-guarantee-immutability-to-remain-competitive-ethereum-classic-developer-says [https://perma.cc/ES5J-NM99] (citing Igor Artamonov, *Does Ethereum-Classic has* [sic] *any significance in terms of Technology?*, QUORA (Oct. 9, 2019), https://www.quora.com/Does-Ethereum-Classic-has-any-significance-in-terms-of-Technology/answer/Igor-Artamonov [https://perma.cc/UNU6-A9LL]).

[21] The consensus generally stays unchanged, but it can be done. For instance, Ethereum plans on switching from a Proof of Work consensus to a Proof of Stake consensus in the coming months, with a proposed consensus protocol called Casper.

[22] *See generally* MICHAEL J. CASEY & PAUL VIGNA, THE TRUTH MACHINE: THE BLOCKCHAIN AND THE FUTURE OF EVERYTHING (2018). On the difficulty to define trust, see WERBACH, *supra* note 5, at 20; Annette Baier*, Trust and Antitrust*, 96 ETHICS 231, 231–32 (1986) (discussing different types of trust relationships).

[23] Some simply make a distinction between blockchain as crypto-currencies and blockchain as applications.

[24] MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY 1–8 (2015). *See also infra* Appendix 1: Trust by Smart Contracts Through the Existence of Collusion.

[25] Ethereum, *A Next-Generation Smart Contract and Decentralized Application Platform*, GITHUB, https://github.com/ethereum/wiki/wiki/White-Paper [https://perma.cc/G72K-YUVJ] (describing smart contracts as "complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules."). For an overview of how smart contracts work, see Kevin Werbach & Nicolas Cornell, *Contracts* Ex Machina, 67 DUKE L.J. 313, 319–24 (2017).

social media, online research, and more.[26] These three usages of blockchain come with different challenges for antitrust authorities, with collusive agreements as a major challenge.

B. The Practice: Collusive Agreements' State of the Art

The antitrust and competition law literature on monopolization and abuses of dominant positions is highly polarized as some authors dispute the harmful nature of such practices.[27] This is not the case with the literature dealing with collusive agreements. It has been said that "[n]o modern development in antitrust law is more striking than the global acceptance of a norm that condemns cartels as the markets most dangerous competitive vice."[28]

Here, the term "collusive agreements" "describe[s] the economic nature of the behavior rather than how it might be categorized under the law."[29] They encompass agreements and concerted practices, as well as cartels and vertical agreements. These concepts refer to different forms of anti-competitive practices and constitute the vast majority of cases decided by the Federal Trade Commission ("FTC"), the Department of Justice ("DOJ"), and the European Commission, other than merger investigations. In the absence of clear definitions, a broad meaning has been given to the terms "agreement," "decision," and "concerted practice,"[30] which generates a large amount of litigation. For this reason among others, the European Commission has not sanctioned any abuse of dominance between 1991 and 2004,[31] focusing all of its attention on

[26] *See* SWAN, *supra* note 24, at 29–70. Generally speaking, blockchain 3.0 differs from other digital services in that the information generated by the use of the service is not saved on a central server. Instead, a complete copy of the ledger is stored on the users' computers. Moreover, the service is not offered by a single economic agent who acts as an intermediary, but rather is allowed in a distributed way by the blockchain which acts as a platform without being an intermediary.

[27] This has been true since the appearance of the Chicago School. S*ee generally* ROBERT H. BORK, THE ANTITRUST PARADOX: A POLICY AT WAR WITH ITSELF (Basic Books 1978) (discussing the positive impact of monopolization practices on the consumer).

[28] William E. Kovacic, *The Value of Policy Diversification in Cartel Detection and Deterrence*, at 2, ORG. FOR ECON. CO-OPERATION & DEV. [OECD] ROUNDTABLE ON EX OFFICIO CARTEL INVESTIGATIONS AND THE USE OF SCREENS TO DETECT CARTELS, DAF/COMP(2013)22 (Oct. 24, 2013).

[29] LOUIS KAPLOW, COMPETITION POLICY AND PRICE FIXING 34 (2013). *See also* Joseph E. Harrington, Jr., Developing Competition Law for Collusion by Autonomous Price-Setting Agents 2 (Aug. 22, 2017) (unpublished manuscript), https://ssrn.com/abstract=3037818 [https://perma.cc/7RKY-DNY3] ("[C]ollusion is when firms use strategies that embody a reward-punishment scheme which rewards a firm for abiding by the supracompetitive outcome and punishes it for departing from it.").

[30] RICHARD WHISH & DAVID BAILEY, COMPETITION LAW 101–02 (Oxford Press 9th ed. 2018).

[31] *See* THIBAULT SCHREPEL, L'INNOVATION PREDATRICE EN DROIT DE LA CONCURRENCE 360 (Bruylant 2018).

clearing up the jurisprudence related to collusive agreements. As a result, on both North American and European soil, collusive agreements are the subject of extensive case law.[32]

A new question awaits to be answered: will blockchain shuffle the cards again? Will this technology change the nature or form of collusive agreements from which the markets suffer, this "supreme evil of antitrust?"[33] Blockchain can be used as a medium for these collusive agreements, or even be the subject of an agreement in itself, depending on the conditions of entry, use, and exit from the technology. To answer these questions, one must review the literature on the functions of collusive agreements as well as the definition of cooperative games within game theory.[34]

"The fundamental distinction between cooperative and noncooperative games is that cooperative games allow binding agreements while noncooperative games do not."[35] Collusion is generally enforced without using (legally) binding agreements, and for that reason, is seen as an outcome of noncooperative games which respond to well-known and identifiable patterns.[36] But in fact, companies achieve the highest (illegal) gain when they trust each other,[37] often making it difficult for the regulator to identify these practices. Trust tends to direct the players toward a more cooperative outcome because it pushes them to accept being vulnerable vis-à-vis someone else, and when the players cooperate effectively, detection is complicated.[38]

What these basic principles of game theory typically do not show is the importance of the medium in which the game is played. Blockchain can play a key role in this respect by allowing more co-operation between the players. The question then becomes whether blockchain can be used to set up a system of binding agreements, and accordingly, to change the game into a cooperative one.

[32] See U.S. DEP'T OF JUSTICE, ANTITRUST DIV., WORKLOAD STATISTICS FY 2009–2018, https://www.justice.gov/atr/file/788426/download [https://perma.cc/75A5-ADRY]. Also, a study of federal antitrust class action cases filed between January 1, 2007 and December 31, 2009 shows that 80% of the cases asserted Section 1 claims, *see* William Kolasky, *Anti-Trust Litigation: What's Changed in Twenty-Five Years?*, 27 ANTITRUST 9, 10 (2012).

[33] Verizon Commc'ns v. Law Offices of Curtis V. Trinko, 540 U.S. 398, 408 (2004).

[34] Defined here as the study of mathematical models for projecting scenarios between players.

[35] KAPLOW, *supra* note 29, at 177 (citations omitted).

[36] Only if the colluders were to use legally binding contracts to enforce the collusion would it make sense to analyze the agreement with cooperative game theory.

[37] *See* Christopher R. Leslie, *Antitrust Amnesty, Game Theory, and Cartel Stability*, 31 J. CORP. L. 453, 462 (2006) ("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 & James T. Tedeschi, *Strategy and the Credibility of Promises in the Prisoner's Dilemma Game,* 12 J. CONFLICT RESOL. 224, 226 (1968); David M. Messick et al., *Individual Adaptations and Structural Change as Solutions to Social Dilemmas*, 44 J. PERSONALITY & SOC. PSYCHOL. 294 (1983).

[38] Leslie, *supra* note 37, at 177.

Coupled with smart contracts, blockchain makes it possible to automate transactions between players and to transform certain noncooperative games into cooperative games in which the initial agreement of the players is ensured by technology and seen as an alternative system for contract enforcement.[39] Combined with smart contracts, blockchain makes colluders trust each other because the terms of the agreement are immutable.[40] Moreover, to the extent that the technology allows for binding agreements, the need to rely on the threat of punishment strategies diminishes, which make collusive outcomes more stable when compared to such outcomes in noncooperative games. It also makes the players less vulnerable vis-à-vis competition agencies. Precisely because companies can generate more illegal profits when they trust each other,[41] competition and antitrust agencies' task is to create a prisoner's dilemma in which each player shares the same dominant strategy: to denounce the agreement.[42] Blockchain can help the players to build a reserve of trust, which in turn requires a greater effort from competition agencies.

The legal framework in which the game is played may also change the outcome of the game.[43] The destabilization strategies created by legislators can modify the behavior of the players involved in a collusive agreement. From 1995–2009, the European Union and the United States introduced significant changes to their policies on the discovery, prosecution, and punishment of cartels.[44] Introduced in 1978 by the United States DOJ [45] and in 1996 by the European Commission,46 the leniency procedure by which colluders self-report their practice and hand over evidence is key in detecting, investigating, and prosecuting

[39] *See* Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 374–75 (2016) (highlighting that blockchain could integrate mechanisms allowing tacit coordination games).

[40] *See infra* Appendix 1.

[41] G. Richard Shell, *Opportunism and Trust in the Negotiation of Commercial Contracts: Toward a New Cause of Action*, 44 VAND. L. REV. 221, 225–26 (1991).

[42] *See infra* Section IV.B.

[43] *See* Michael Saller, *Challenges and Co-Ordination of Leniency Programmes - Background Note by the Secretariat*, at 6, ORG. FOR ECON. CO-OPERATION AND DEV. [OECD] WORKING PARTY NO. 3 ON CO-OPERATION AND ENFORCEMENT, DAF/COMP/WP3(2018)1 (June 3, 2008), ("A functioning leniency programme creates a 'prisoner's dilemma' because all participants will fear that one of them will come forward and report the cartel to the authorities, securing immunity or at least a significant reduction of the fines for itself, at the expense of the other participants of the cartel who will suffer high(er) sanctions.").

[44] *See* Joseph E. Harrington, Jr. & Myong-Hun Chang, *Modeling the Birth and Death of Cartels with an Application to Evaluating Competition Policy*, 7 J. EUR. ECON. ASS'N. 1400, 1419–20 (2009).

[45] Org. for Econ. Co-operation and Dev. [OECD], *Leniency for Subsequent Applicants*, at 9, DAF/COMP(2012)25 (Oct. 2012) ("In 1978 the US Department of Justice (US DoJ) adopted its first Corporate Leniency Policy in an attempt to overcome these limitations and enhance deterrence.").

[46] *Id.* at 10 ("In 1996, the European Commission (EC) adopted its first Leniency Notice.").

hard-core cartels as well as other types of collusion. Over the years, leniency has become the "most effective tool in the fight against cartels."[47]

According to the European Commission, "the leniency policy proves very successful in fighting cartels."[48] By the same token, the DOJ stated that "[t]he Program (and its counterpart for individual leniency applicants) has been an incredible success in deterring and detecting antitrust crimes."[49] It is the "most important investigative tool for detecting cartel activity."[50] It has been shown that anti-cartel enforcement influences firms' behavior[51] and may be influential in deterring low-overcharge cartels as well as high-overcharge cartels.[52] I shall therefore address whether the success of leniency applications is put into danger by blockchain; in other words, whether the technology limits the destabilization of game strategies. I shall then discuss whether this would be problematic. Several studies estimate that the percentage of detected cartels is only between 10% and 33% in the post-World War II era,[53] which proves that leniency procedures are not sufficient in themselves. Perhaps antitrust and competition agencies give leniency procedures too much importance, which the blockchain will help to correct. And if only 12% of cartels end naturally (meaning that they end by themselves, mostly because of internal disagreements),[54] blockchain may change that too.

C. Blockchain and Collusive Agreements: New Challenges

Algorithmic collusive agreements are increasingly discussed.[55] Much of the literature deals with how collusive agreements are carried

[47] *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.

[48] *Cartels: Leniency,* EUROPEAN COMM'N: COMPETITION, http://ec.europa.eu/competition/cartels/leniency/leniency.html [https://perma.cc/ZM33-KWUF].

[49] *Silver Anniversary: The Antitrust Division's Leniency Program Turns 25*, U.S. DEP'T OF JUSTICE, https://www.justice.gov/atr/division-operations/division-update-spring-2018/antitrust-division-leniency-program-turns-25 [https://perma.cc/9Q8B-QVBB].

[50] *Leniency for Subsequent Applicants*, *supra* note 45, at 152.

[51] *See* Michael Kent Block et al., *The Deterrent Effect of Antitrust Enforcement*, 89 J. POL. ECON. 429, 434 (1981).

[52] Iwan Bos et al., Does Enforcement Deter Cartels? A Tale of Two Tails 32 (Mar. 1, 2017) (unpublished manuscript), https://ssrn.com/abstract=2471425 [https://perma.cc/58R7-A6K5]. In low-overcharge cartels, the colluders agree on a price that is right above the competitive price. In high-overcharge cartels, they agree on a price that is way above the competitive price.

[53] John M. Connor, *Cartel Detection and Duration Worldwide*, CPI ANTITRUST CHRON., Sept. 2011, at 2.

[54] Margaret C. Levenstein & Valerie Y. Suslow, *What Determines Cartel Success?*, 44 J. ECON. LIT. 43, 51 (2006).

[55] *See, e.g.*, Frédéric Marty, *Intelligence Artificielle et Organisation Industrielle: Quels Enjeux pour l'Économie Numérique* 2–13 (Groupe de recherche en Droit, Economie et Gestion, Working Paper No. 2018-21).

out.[56] But too little is said about the content of the agreements, as well as the medium on which they take place. Studying algorithmic agreements without taking their medium into account is equivalent to analyzing the market for smartphone apps without taking into account how operating systems work. Such an analysis is incomplete and runs the risk of being unproductive.

To address this shortfall, this Article will discuss the different types of algorithmic collusive agreements that blockchain allows, and whether the technology permits more or longer collusive agreements. It will further analyze the extent to which blockchain protects collusive agreements from competition and antitrust authorities while creating transparency between colluders, in other words, whether blockchain provides companies with better means of coordination. This Article will then address if smart contracts could allow efficient exit from collusive agreements, thereby bypassing enforcement by antitrust and competition agencies.

Most of the literature focuses on how the law is influencing companies' behaviors, but that only tells part of the story, as the technology may also be used by companies to fight back against the distrust created by the law. This Article aims to fill the gap by analyzing to what extent blockchain allows the creation of trust between colluders despite the law. One may indeed wonder if blockchain will cause an increase in the number of collusive agreements, and if these agreements will be more robust than those created outside the blockchain.[57] In other words, will blockchain create an environment conducive to the survival of collusive agreements? Will new types of such agreements emerge? Will they be more or less harmful to consumers than current ones? Will they be more or less easy to detect? If they are detected, will the remedies be enforceable? More generally, will the impact of blockchain on collusive agreements lead antitrust and competition agencies to change their approach, and more substantially, their role?

Answers to these questions are necessary because blockchain must be free from monopolization, abuses of dominance, and collusive agreements to produce the maximum good. Answering these questions requires an in-depth analysis of two pillars. The first is substantive. Blockchain challenges law enforcement by making it possible to im-

[56] *See, e.g.*, Harrington, Jr., *supra* note 29; Levenstein & Suslow, *supra* note 54; Yuliya Bolotova et al., Cartel Stability: An Empirical Analysis (Oct. 2006) (unpublished manuscript), https://ssrn.com/abstract=939078 [https://perma.cc/4KKS-N845].

[57] The issue of collusive agreements is not the only antitrust issue relevant to blockchain. An earlier study by the author of this Article dealt with the impact of blockchain on monopolization and abuses of dominance. *See generally* Thibault Schrepel, *Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox*, 3 GEO. L. TECH. REV. 281 (2019) (analyzing how the technology will challenge existing dominant positions, but also, how it will give rise to monopolization and abuses of dominance).

plement illegal practices more efficiently with the help of smart contracts. The contours of what the technology allows must therefore be precisely defined. The second is procedural. Blockchain challenges the law's enforceability because of its technical characteristics. Blockchain is pseudonymous and immutable, which creates issues regarding the detection of practices as well as the identification of perpetrators. I will address these two pillars by studying the birth of collusive agreements through blockchain, their life, and their death.

II. The Birth of Collusive Agreements on Blockchain

Blockchain may be used to facilitate the creation of collusive agreements. A distinction between two types of agreements is to be made: agreements that directly concern the conditions of access, use, and/or exit from the blockchain, and agreements that are created outside the blockchain which use the technology to make the agreements more efficient. This Part explores both.

To this end, I will detail not only how this technology can be used to facilitate agreements as we know them, but also what new strategies may be implemented on this technology. I will discuss which blockchain parameters give rise to certain types of collusion, on which types of blockchain, using which mechanisms, and under which types of smart contracts (if any).

A. Collusive Agreements Related to Blockchain

I will successively discuss collusive agreements concerning the conditions of access, use, and/or exit from blockchains themselves. The first type of such agreements concerns public blockchains, the second type deals with private blockchains, and the third type relates to the mechanisms chosen on a blockchain, regardless of whether the blockchain is public or private. I will show that while the existing case law provides some answers to the questions raised by blockchain in this field, many of the issues remain unanswered.

1. Collusive Agreements Related to Public Blockchain

Consider the following situation which may be illustrative when discussing collusive agreements related to public blockchain:

Two companies use a public blockchain to facilitate the exchange of information between them. Because the blockchain is public, the two companies are under the impression that they are not operating a secret exchange of confidential information. The blockchain uses "Proof of Stake" to achieve the distributed consensus. This consensus mechanism ensures integrity as well as the absence of absolute control by one of *the two companies. The relevant competition agency is alerted by a competitor to the exchange of information going on between the two companies.*

This Section questions whether blockchain can in itself qualify as a collusive agreement, without further analyzing the information contained within a blockchain or the use made of that blockchain. Analyzing whether the mere creation or use of a public blockchain can violate antitrust or competition law leads to questioning two points. First, one may ask whether the creation of a blockchain as a medium for future exchanges can be addressed by antitrust and competition law. Second, one must study the extent to which the purpose(s) that led to the creation of a public blockchain can be used to characterize an illegal agreement.

Regarding the analysis of blockchain as a medium, in the United States, Section 1 of the Sherman Act states that "[e]very contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal."[58] The term "agreement" is not defined, but it is clear from the case law that an agreement does need not to be a formal written document.[59] The United States Supreme Court has held that companies have entered into an illegal agreement when "the possibility of independent action" is excluded and when they "had a conscious commitment to a common scheme."[60] Parties can meet these two criteria by agreeing to create and use a blockchain.

In Europe, Article 101(1) of the Treaty on the Functioning of the European Union ("TFEU") provides that "all agreements between undertakings, decisions by associations of undertakings and concerted practices that may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market" are prohibited.[61] In other words, illegal practices are prohibited, but the medium allowing these practices is not. Accordingly, could the creation of a blockchain be considered an agreement, a decision by associations of undertakings, or a concerted practice?[62]

Agreement. The jurisprudence holds that the proof of an agreement must be founded upon the direct or indirect finding of "the existence of

[58] 15 U.S.C. § 1 (2018).

[59] *See* George A. Hay, *The Meaning of "Agreement" Under the Sherman Act: Thoughts from the "Facilitating Practices" Experience*, 16 REV. INDUS. ORG. 113 (2000).

[60] Monsanto v. Spray-Rite Serv. Corp., 465 U.S. 752, 768 (1984).

[61] Consolidated Version of the Treaty on the Functioning of the European Union art. 101(1), May 9, 2008, 2008 O.J. (C 115) 47, 88–89.

[62] These three qualifications are overlapping and nothing indicates that one practice should result from one or the other as they are collectively used to prohibit anti-competitive agreements.

the subjective element that characterizes the very concept of an agreement, that is to say a concurrence of wills between economic operators on the implementation of a policy, the pursuit of an objective, or the adoption of a given line of conduct on the market."[63] The fact that several companies create a blockchain, or share information on it, could therefore be seen as an agreement because by doing so, they are expressing their joint intention to conduct themselves on the market in a specific way. The concurrence of wills is characterized by the willingness to share information on the same blockchain.

Association. A blockchain could also constitute a decision by associations of undertakings, although only anti-competitive decisions emanating from these associations are punished. The question is whether the mere creation of a blockchain for anti-competitive purposes, or the sharing of information on a public blockchain may be characterized as a decision whose intention is to coordinate all users' actions. It appears to be theoretically possible.

Concerted practices. Lastly, could blockchain be seen as a concerted practice? According to European jurisprudence, concerted practices are characterized by the "coordination between undertakings which, without having reached the stage where an agreement properly so-called has been conducted, knowingly substitutes practical co-operation between them for the risks of competition."[64] They are a "safety-net catching looser forms of collusion."[65] The European Court of Justice further holds that Article 101 precludes

> direct or indirect contact between such operators, the object or effect whereof is either to influence the conduct on the market of an actual or potential competitor or to disclose to such a competitor the course of conduct which they themselves have decided to adopt or contemplate adopting on the market.[66]

Interestingly, the European General Court has considered that even the unilateral disclosure of information that is relevant to the market may constitute a concerted practice,[67] which is exactly what sharing information on a public blockchain entails. Public blockchains could also be used to discourage companies — especially small ones — from offering prices other than those of competitors, because if they do, the

[63] Case T-41/96, Bayer v. Comm'n, 2000 E.C.R. II-3383, ¶ 173.

[64] Case 48/69, Imperial Chemical Industries Ltd. v. Comm'n, 1972 E.C.R. 619, ¶¶ 64–65.

[65] ALISON JONES & BRENDA SUFRIN, EC COMPETITION LAW: TEXT, CASES AND MATERIALS 173 (3d ed. 2007).

[66] Case C-40/73, Suiker Unie v. Comm'n, 1975 E.C.R. 1663, ¶ 174.

[67] Joined Cases T-202/98, T-204/92 & T-207/98, Tate & Lyle plc v. Comm'n, 2001 E.C.R. II-2040, ¶ 35, 54, 61.

information will be shown to everyone. As a consequence, provided that an anti-competitive object or effect is shown, a public blockchain could in itself constitute a cartel.

In short, the mere creation or use of a public blockchain can be seen as the implementation of a medium for future anti-competitive practices. Blockchain, as a technology, does not escape antitrust and competition law. One may then analyze whether creating a public blockchain to exchange information could be illegal. To this end, the public nature of blockchain plays an important role.

In the United States, the exchange of public information is generally not considered an infringement of competition rules. In earlier decisions, the Supreme Court was concerned with such exchanges of public information including "suggestions as to both future prices and production."[68] Following *United States v. United States Gypsum Co.*, in which the Supreme Court noted that agreements to exchange information were evaluated under the rule of reason, the case law now focuses on actual evidence of anti-competitive harm.[69] When information is publicly available, "the risk of its exchange between competitors seems low."[70] Because the plaintiff bears the initial burden of proof to show that the agreement to exchange information led to substantial anti-competitive effects in a relevant market, the mere creation of a blockchain is unlikely to be seen as illegal in the U.S. In other words, blockchain is an agreement, but it is not automatically an unlawful agreement absent some combination of intent and effects on competition in the relevant market.

In Europe, the Horizontal Guidelines provide that "in general, exchanges of genuinely public information are unlikely to constitute an infringement of Article 101."[71] The Guidelines further add that "*genuinely public information* is information that is generally equally accessible (in terms of costs of access) to all competitors and customers" and that "[f]or information to be genuinely public, obtaining it should not be more costly for customers and companies unaffiliated to the exchange system than for the companies exchanging the information."[72]

[68] Am. Column & Lumber Co. v. United States, 257 U.S. 377, 399 (1921).

[69] United States v. U.S. Gypsum Co., 438 U.S. 422, 438 (1978).

[70] Org. for Econ. Co-operation and Dev. [OECD], *Information Exchanges Between Competitors under Competition Law*, at 296, DAF/COMP(2010)37 (July 11, 2010). In fact, "[c]ompetition does not become less free merely because the conduct of commercial operations becomes more intelligent through the free distribution of knowledge of all the essential factors entering into the commercial transaction." Maple Flooring Mfrs. Ass'n. v. United States, 268 U.S. 563, 583 (1925). For a list of all criteria used to characterize an illegal exchange of information, see Spencer W. Waller, *Trade Associations, Information Exchange, and Cartels*, 30 LOY. CONSUMER L. REV. 203, 206–07 (2018).

[71] *Guidelines on the Applicability of Article 101 of the Treaty on the Functioning of the European Union to Horizontal Co-operation Agreements*, ¶ 92, COM (2011) C 11/1 (Jan. 14, 2011).

[72] *Id*.

This is exactly what blockchain does; it turns private information into genuinely public information. These Guidelines do not provide full exemption from competition law and we must further analyze what kind of information is being shared.

The European jurisprudence holds that public information sharing only constitutes a cartel when the information concerns future prices[73] or strategies.[74] The sharing of actual prices constitutes a "market behavior which does not lessen each undertaking's uncertainty as to the future attitude of its competitors. At the time when each undertaking engages in such behavior, it cannot be sure of the future conduct of the others."[75] As a matter of fact, I have not identified any jurisprudence sanctioning the mere fact of publicly sharing actual prices as such practice does not restrict companies' freedom to determine their market behavior independently.[76] Indeed, the jurisprudence holds that shared data must be "ultimately aimed at reducing or eliminating uncertainty as to the future pricing behavior of parties."[77] This is confirmed in the European Commission Guidelines on the applicability of Article 101 to horizontal co-operation agreements, which refers to information reducing "strategic uncertainty."[78] In short, the data must be of such a nature that the company cannot refrain from taking it into account when defining its market behavior.[79]

[73] *Id.* ¶ 74. *See generally* Joined Cases T-25/95, T-26/95, T-30/95, T-31/95, T-32/95, T-34/95, T-35/95, T-36/95, T-37/95, T-38/95, T-39/95, T-42/95, T-43/95, T-44/95, T-45/95, T-46/95, T-48/95, T-50/95, T-51/95, T-52/95, T-53/95, T-54/95, T-55/95, T-56/95, T-57/95, T-58/95, T-59/95, T-60/95, T-61/95, T-62/95, T-63/95, T-64/95, T-65/95, T-68/95, T-69/95, T-70/95, T-71/95, T-87/95, T-88/95, T-103/95 & T-104/95, Cimenteries CBR v. Comm'n, 2000 E.C.R. ¶ 1531; Joined Cases C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P & C-219/00P, Aalborg Portland A/S v Comm'n, 2004 E.C.R. I-123.

[74] *Guidelines on the Applicability of Article 101*, *supra* note 71, at 92. *See* Joined Cases T-25/95, T-26/95, T-30/95, T-31/95, T-32/95, T-34/95, T-35/95, T-36/95, T-37/95, T-38/95, T-39/95, T-42/95, T-43/95, T-44/95, T-45/95, T-46/95, T-48/95, T-50/95, T-51/95, T-52/95, T-53/95, T-54/95, T-55/95, T-56/95, T-57/95, T-58/95, T-59/95, T-60/95, T-61/95, T-62/95, T-63/95, T-64/95, T-65/95, T-68/95, T-69/95, T-70/95, T-71/95, T-87/95, T-88/95, T-103/95 & T-104/95, Cimenteries CBR v. Comm'n, 2000 E.C.R. ¶ 1531 (regarding price intention); Joined Cases C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P & C-219/00P, Aalborg Portland A/S v Comm'n, 2004 E.C.R. I-123. With regard to natural capacity increases, *see* Commission Decision 72/474, 1972 O.J. (L 303/24); Commission Decision 84/405, 1984 O.J. (L 220/27) (regarding investment plans).

[75] Joined Cases C-89/85, C-104/85, C-114/85, C-116/85, C-117/85 & C-125–129/85, Ahlström Osakeyhtiö v. Comm'n, 1996 E.C.R. I-1307, ¶ 64; *see also Information Exchanges Between Competitors*, *supra* note 70, at 28, 29, 165. Furthermore, *see generally* Org. for Econ. Co-operation and Dev. [OECD], *Unilateral Disclosure of Information with Anticompetitive Effects*, at 20, DAF/COMP(2012)17 (Oct. 11, 2012); Cases T-191/98 & T-212–214/98, Atlantic Container Line v. Comm'n, 2003 E.C.R. II-3275, ¶ 1154.

[76] JONES & SUFRIN, *supra* note 65, at 903.

[77] Commission Decision COMP/39.188 of Oct. 15, 2008, Relating to a Proceeding Under Article 81 of the EC Treaty, at 72, C(2008) 5955 final, (2008).

[78] *Guidelines on the Applicability of Article 101*, *supra* note 71, ¶ 61.

[79] NICOLAS PETIT, DROIT EUROPEEN DE LA CONCURRENCE 628 (2nd ed. 2018).

In practice, the burden of proof lies with the Commission, which must prove that the exchange of information constitutes the only plausible explanation of a subsequent parallelism of behaviors.[80] This burden of proof is very high, even though the European Commission may apply the method of *faisceau d'indices* (bundle of indicators).[81] Consequently, there is every reason to believe that a company's sharing of its current prices on a blockchain won't violate as such TFEU Article 101.

As a result, in both the United States and Europe, the mere creation and participation in a public blockchain, without taking its content and specific use into account, should not trigger a sanction under antitrust and competition law.[82]

2. Collusive Agreements Related to Private Blockchain

Consider now the following example, helpful in understanding collusive agreements related to private blockchain:

Three companies agree together on the creation of a blockchain to track food products. This blockchain is private and its access is thus restricted to users who are pre-approved by these three companies. A few months after its creation, several distributors are added to the blockchain. But soon after, following a disagreement over the blockchain mechanisms, the three companies unanimously decide to exclude one of these distributors from it.

In this example, neither the information exchanged on the blockchain nor the use of the blockchain is anti-competitive, but the conditions of access to the blockchain may very well be. One could imagine another situation in which the conditions of use are anti-competitive and give rise to an illegal agreement between companies. This could be the case if one company participating in the blockchain does not have access to part of the blockchain.[83] But in this example, again, it is only the blockchain's design that may raise anti-competitive concerns.

The occurrence of such an anti-competitive agreement is highly likely. Blockchains are generally made private so their creators can regulate their use. In the example, the three creators agreed to exclude one user from it. In terms of antitrust and competition law, this practice

[80] Case T-65/89, BPB Industries plc v. Comm'n, 1993 E.C.R. II-389.

[81] Joined Cases T-44/02, T-54/02, T-56/02, T-60/02 & T-61/02, Dresdner Bank AG v. Comm'n, 2006 E.C.R. II-3567, ¶¶ 64–67.

[82] JONES DAY, *supra* note 13, at 3 ("The formation of a blockchain, without more, cannot result in antitrust liability.").

[83] "If private blockchain members exclude competitors from accessing a blockchain that has become essential to doing business, nonmembers may not be able effectively to compete." *Id.* at 3–4. This, for instance, is made possible by Layer 2 systems, which provide ways to limit the amount of information released to the public. *See* Johann Palychata, *Blockchain: Time for an upgrade? Where to look in the next 6 months*, LINKEDIN (Oct. 16, 2018), https://www.linkedin.com/pulse/blockchain-time-upgrade-where-look-next-6-months-johann-palychata [https://perma.cc/N2MF-8GXJ].

would only be illegal if the blockchain is used for purposes other than anti-competitive ones,[84] and also in the United States, if the defendants have "market power or exclusive access to an element essential to effective competition."[85] To this extent, the exclusion from the blockchain may then constitute a concerted refusal to deal or a market allocation to the extent that the colluders will be able to use the information on the ledgers to adapt their strategy.[86]

Additionally, exclusion from a blockchain may constitute an abuse of collective dominance on European soil,[87] which falls within the scope of TFEU Article 102. This is found where collectively dominant firms enjoy some structural or contractual link, or when they are active in a market that otherwise allows them to coordinate their behavior.[88] In short, the case law finding collective dominance is based on agreements between firms allowing them to behave as a collective entity. The decision to exclude one user from the blockchain could be seen as being such an agreement. However, the case law punishing such abuses remains scarce.[89]

3. Collusive Agreements by Consensus Mechanisms

Consider the following scenario, useful for understanding collusion regarding blockchain functioning:

A company creates a new blockchain to divide the market with its competitors on the basis of shared information. It first wonders which consensus mechanism would be best suited for this practice, and for that, studies the various consensuses to assess which one allows control of the blockchain between cartelists. The company's intention is not to ensure the integrity of the blockchain, but to ensure that some users

[84] The exclusion of a user from an illegal practice cannot be punished in itself. *See generally* Karen Yeung, *Regulation by Blockchain: The Emerging Battle for Supremacy between the Code* of *Law and Code* as *Law,* 82 MOD. L. REV. 207 (2019). On per se prohibition of a service in the United States, see MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 914, 919 (2005) (holding that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties").

[85] *See* Northwest Wholesale Stationers, Inc. v. Pacific Stationery and Printing Co., 472 U.S. 284, 296 (1985).

[86] Here, the analysis concerns both the use and the creation of the blockchain itself.

[87] *See* Case T-193/02, Piau v. Comm'n, 2005 E.C.R. II-209, ¶ 118.

[88] The ongoing debate regarding minority shareholdings should be mentioned here. *See* Einer Elhauge, *How Horizontal Shareholding Harms Our Economy—And Why Antitrust Law Can Fix It* (Harvard Olin Center, Discussion Paper No. 982, Dec. 2018) (arguing that horizontal shareholdings harm the economy). *But see* Thomas A. Lambert & Michael E. Sykuta, *The Case for Doing Nothing About Institutional Investors' Common Ownership of Small Stakes in Competing Firms*, 13 VA. L. & BUS. REV. (forthcoming 2019); Org. for Econ. Cooperation and Dev. [OECD], *Common Ownership by Institutional Investors and its Impact on Competition*, at 6, DAF/COMP(2017)1 (Dec. 5–6, 2017).

[89] *See* PETIT, *supra* note 79, at 411.

may — despite the overall number of other users — control the blockchain for their own interests.

The issue here is to evaluate the antitrust risk implied by certain consensus mechanisms, and more generally, by certain mechanisms of blockchain. Three different groups may have sufficient power to organize a cartel: miners (including validators), users, and core developers. The risk created by such power must be taken into account by the antitrust and competition authorities, particularly when creating safe harbors.[90]

a. Regarding the Miners

Blockchain mining involves adding transactions to an existing blockchain. On widely used blockchains, many transactions are added, and as a consequence, the power of each miner is minimal. The situation is different when miners are grouped in a pool where the profit generated by the mining activity is shared according to the hashing power provided by each miner.[91] The incentive to join such pools leads to rapid expansion. As a result, fewer than ten mining pools dominated Bitcoin in 2017. In fact, the seven most powerful pools accounted for more than 85% of all transactions validated on the Bitcoin blockchain.[92] This dominance calls into question the proclaimed decentralized nature of Bitcoin because ownership of more than 51% of the mining power is equivalent to control of the blockchain.[93]

Only a change in the blockchain consensus may redistribute mining power.[94] Consensus mechanisms differ from one another in how the blocks are validated, but differ very little on how users can read information and register new transactions. It follows that the integrity of blockchains is at stake, not their functioning. For that reason, none of them should be found anti-competitive per se, and yet, several blockchains tend to facilitate the emergence of anti-competitive practices,[95]

[90] Safe harbors, according to which certain practices are deemed not to violate the law, should not be granted to individuals when the risks of them committing an illegal practice is high.

[91] WERBACH, *supra* note 5, at 120.

[92] *See Hashrate Distribution*, BLOCKCHAIN https://www.blockchain.com/pools [https://perma.cc/4USA-DZP3].

[93] WERBACH, *supra* note 5, at 119.

[94] Changing the consensus mechanism may be desirable to undermine mining pools' power. For instance, several pools threatened to create hard forks during the Bitcoin block size controversy. *See* David Dinkins, *Satoshi's Best Kept Secret: Why is There a 1 MB Limit to Bitcoin Block Size*, COINTELEGRAPH (Sept. 19, 2017), https://cointelegraph.com/news/satoshis-best-kept-secret-why-is-there-a-1-mb-limit-to-bitcoin-block-size [https://perma.cc/6VWW-VF53].

[95] Do miners and/or validators form a single economic entity? If that is the case, they are not separate undertakings and, as a consequence, there is no possible collusion between them. *See* Ionnis Lianos, *Blockchain Competition,* at 84 (Univ. Coll. London, Ctr. for Law, Econ. & Soc'y, Research Paper 8/2018, Sept. 2018).

leading to a "cartel capture" of blockchain governance. Indeed, these pool miners are often physically together, which allows them to learn each other's real-life identities, and therefore, to coordinate their behaviors.[96]

Unlike practices whose effects occur outside the blockchain, collusion regarding the blockchain only produces direct effects inside the technology ecosystem, thus greatly reducing the detection risk. Antitrust and competition authorities must therefore be particularly vigilant and focus their efforts where the risk is greatest. Not all consensus mechanisms have the same risk level. Accordingly, the goal here is to identify the main consensus mechanisms currently in use and to draw some general lessons to be applied to the new consensus mechanisms that will be developed in the years to come.[97]

Using Proof of Work, miners compete to add a set of transactions — gathered as a block — in the chain by racing to solve a cryptographic puzzle.[98] The first to solve it wins the lottery and is rewarded by receiving a transaction fee as well as newly minted tokens. Thanks to Bitcoin, this is currently the world's most used consensus mechanism.[99] It has the advantage of allowing a relatively random distribution of block validation operations, which limits the risk of collusion, but suffers from the power the mining requires[100] as well as scaling issues.[101]

Using Proof of Stake, the chances for one user to validate blocks increase with the number of tokens the user owns in the system. One user with 200 tokens will be twice as likely to be selected as another user with 100 tokens. There is no coin creation (mining) in Proof of Stake, so validators are exclusively rewarded in transaction fees. Once a block is created, it has to be committed to the blockchain. Different systems are in use: some choose a random group of signers, while others require a majority.[102] In any case, validators have nothing to lose —

[96] For an example of miners coordinating their behavior through a pool, see Kristian Soltes, *The First Blockchain Antitrust Case. Or Is It?*, CONSTANTINE CANNON (May 29, 2019), https://constantinecannon.com/2019/05/29/the-first-blockchain-antitrust-case-or-is-it [https://perma.cc/NG3X-S3LS].

[97] Please note that only the most commonly used consensus mechanisms are analyzed here. Many others will be created in the years to come and will also deserve an assessment.

[98] Schrepel, *supra* note 57, at 292.

[99] *See* Andrew Tar, *Proof-of-Work, Explained*, COINTELEGRAPH (Jan. 17, 2018), https://cointelegraph.com/explained/proof-of-work-explained [https://perma.cc/2TCU-XJVZ].

[100] *But see* Vladimir Jelisavcic, *Bitcoin Uses a Lot of Energy, But Gold Mining Uses More*, LONGHASH (Sept. 13, 2018), https://www.longhash.com/news/bitcoin-uses-a-lot-of-energy-but-gold-mining-uses-more [https://perma.cc/QV8E-GVYW].

[101] *See* Connor Blenkinsop, *Blockchain's Scaling Problem, Explained*, COINTELEGRAPH (Aug. 22, 2018), https://cointelegraph.com/explained/blockchains-scaling-problem-explained [https://perma.cc/PXZ4-J9XM].

[102] Amy Castor, *A (Short) Guide to Blockchain Consensus Protocols*, COINDESK (Mar. 4, 2017), https://www.coindesk.com/short-guide-blockchain-consensus-protocols

"nothing-at-stake" — and can create two blocks and claim two sets of transaction fees. Fraudulent practices can thus be committed more easily than under Proof of Work.

Under Proof of Activity, Proof of Work and Proof of Stake are combined.[103] First, miners race to solve a cryptographic puzzle. The formed blocks do not contain any transactions, but simply act as a template. The system then switches to Proof of Stake. A randomly selected group of validators sign the new block, knowing that validators with more tokens are more likely to be chosen. The fees are then split up between the miner and the validators who signed off on the block. This mechanism can therefore encourage (illegal) agreements between users who have a high computing speed (those who will likely win the race) and those who have many tokens.

Using Proof of Burn, users "burn" coins or tokens by sending them to an address where they are irretrievable.[104] The more coins or tokens one user sends, the more likely it is for that user to be selected to mine new blocks. The integrity of this consensus mechanism is therefore in the hands of its most powerful users, increasing the risk of collusion because those users operate and effectively control this type of blockchain. Therefore, Proof of Burn facilitates the occurrence of anti-competitive practices.

Using Proof of Capacity, hard drive space is key.[105] For a user, the more hard drive space he has, the better his chances are for mining the next block and earning a reward. Again, the integrity of the system may rest entirely in the hands of those with the most resources (capacity), creating an incentive for implementing collusive agreements knowing that such collusions would be run efficiently.

Using Proof of Elapsed Time, the algorithm uses a trusted execution environment to ensure that blocks get produced in a random lottery fashion, without any work coming from the node.[106] Participants are assigned a random amount of time to wait, and the first to complete the waiting time gets to commit the next block. This system is very similar to Proof of Work but consumes less electricity. The random nature of the users in charge of validating the blocks tends to reduce the risk of collusive agreements being implemented greatly.

[https://perma.cc/ER9Q-824B] ("In Tendermint, for example, every node in the system has to sign off on a block until a majority vote is reached, while in other systems, a random group of signers is chosen.").

[103] Iddo Bentov et al., *Proof of Activity: Extending Bitcoin's Proof of Work Via Proof of Stake*, PERFORMANCE EVALUATION REV., Dec. 2014, at 2.

[104] Xiwei Xu, *A Taxonomy of Blockchain-Based Systems for Architecture Design*, PROC. OF THE 2017 IEEE INT'L CONF. SOFTWARE ARCHITECTURE 243, 251 (2017).

[105] Shihab S. Hazari & Qusay H. Mahmoud, *Comparative Evaluation of Consensus Mechanisms in Cryptocurrencies*, INTERNET TECH. LETTERS, May/June 2019, at 1, 3.

[106] *See* Brian Curran, *What is Proof of Elapsed Time Consensus? (PoET) Complete Beginner's Guide*, BLOCKONOMI (Sept. 11, 2018), https://blockonomi.com/proof-of-elapsed-time-consensus [https://perma.cc/53EB-EJ5W].

Further consensus mechanisms will emerge in the coming years. For instance, Bitcoin is interested in Byzantine Fault Tolerant algorithms ("BFT algorithms") other than Proof of Work.[107] The newly adopted consensus mechanism could be one where only verified and validated users (from a coordinating body) would be able to register transactions and view the entire ledger. This consensus is sometimes described as the "minimum viable centralization."[108] It allows greater control of activities by a central unit, and thus, facilitates collusive activities. Steem.it and EOS use delegated Proof of Stake, in which token holders vote for representatives who validate blocks.[109] This mechanism, which allows validators to be chosen, is particularly conducive to collusive agreements.

In the end, two lessons can be learned from collusive agreements between miners. First, the risk of collusive agreements being implemented is high when the big players are miners and/or validators, because they can control the content of transactions as well as the integrity of the entire system.[110] Also, when the big players are identified as such by the community, some may be tempted to bribe them.[111] Second, the risk of collusive agreements is much lower when the miners and validators are chosen randomly because such a system does not guarantee the possibility for colluders to control it.[112] To date, Bitcoin and Ethereum, the world's two leading blockchains, use Proof of Work. The risk of collusive agreements to be created under this consensus is low, although it cannot be eliminated. But things are moving fast in the blockchain world. For instance, Ethereum intends to migrate to Proof of Stake[113] where the antitrust risk is more substantial. Antitrust and competition agencies must be made aware of this risk map so that they can focus on blockchains using mechanisms that make violations of antitrust and competition law more probable.

[107] Using BFT algorithms, a distributed computer network may function correctly despite malicious nodes of the system which are failing or propagating incorrect information to other peers. *See* Brian Curran, *What is Practical Byzantine Fault Tolerance? Complete Beginner's Guide*, BLOCKONOMI (May 11, 2018), https://blockonomi.com/practical-byzantine-fault-tolerance [https://perma.cc/C7LP-G54L].

[108] WERBACH, *supra* note 5, at 54.

[109] Katie Roman, *Understanding EOS and Delegated Proof of Stake*, STEEMIT (Mar. 5, 2018, 2:28 PM) https://steemit.com/eos/@eosgo/understanding-eos-and-delegated-proof-of-stake [https://perma.cc/T72P-RU3C].

[110] For a description of the whale problem, see *Thought Bitcoin Had a Whale Problem? Ethereum is Much Worse*, LONGHASH (Aug. 27, 2018, 5:07 PM), https://www.longhash.com/news/thought-bitcoin-had-a-whale-problem-ethereum-is-much-worse [https://perma.cc/7TZ2-VARV].

[111] YAGA ET AL., *supra* note 13, at 25; *see also* Vitalik Buterin, *On Collusion* (Apr. 3, 2019), https://vitalik.ca/general/2019/04/03/collusion.html [https://perma.cc/6RDF-RQWQ] (detailing the risk of bribery on blockchain).

[112] *See* JONES DAY, *supra* note 13, at 6.

[113] *Ether,* ETHEREUM, https://www.ethereum.org/ether [https://perma.cc/N9MP-SCQP] ("[W]e are planning to switch to Proof of Stake (PoS).").

b. Regarding the Core Developers

The developers working on the blockchain's core software consist of small groups with a great deal of power over the network, notably that of providing the official software to the verification nodes. This is true, for example, of the Ethereum Foundation[114] and the Bitcoin Foundation[115] whose missions are to promote the protocol of their blockchain. The Bitcoin Foundation also operates by paying certain third parties such as the MIT Digital Currency Initiative, Blockstream, and ChainCode Labs for developing the blockchain.[116] The same goes for private blockchains such as Hyperledger and R3, as they have corporate members who fund them and contribute to the code according to well-established governance structures.[117]

Core developers may initiate a soft or hard fork[118] and communicate with miners regarding future changes in the blockchain. Bitcoin uses a mechanism called BIP 9 that allows core developers to probe miners about technical changes.[119] SegWit uses another mechanism called BIP 91.[120] And "[i]n private blockchains, owners or designated blockchain participants have the authority to resolve discrepancies" which "may not be resolved under an objective consensus mechanism," but require unilateral intervention by the owners and/or designated participants.[121] Unilateral interventions create control over the blockchain which will foster collusive agreements.

[114] *See* ETHEREUM, https://www.ethereum.org [https://perma.cc/2FC9-KWM8].

[115] *See* BITCOIN FOUND., https://bitcoinfoundation.org [https://perma.cc/S2UM-GWLU].

[116] Aaron van Wirdum, *Who Funds Bitcoin Core Development? How the Industry Supports Bitcoin's 'Reference Client'*, BITCOIN MAG. (Apr. 6, 2016), https://bitcoinmagazine.com/articles/who-funds-bitcoin-core-development-how-the-industry-supports-bitcoin-s-reference-client-1459967859 [https://perma.cc/N5Y9-8U83].

[117] WERBACH, *supra* note 5, at 121. More generally, on governance and blockchain, see DON TAPSCOTT & ALEX TAPSCOTT, WORLD ECONOMIC FORUM, REALIZING THE POTENTIAL OF BLOCKCHAIN: A MULTISTAKEHOLDER APPROACH TO THE STEWARDSHIP OF BLOCKCHAIN AND CRYPTOCURRENCIES, 7 (June 2017).

[118] Generally speaking, a soft fork is a modification of the software protocol where previously valid blocks are made invalid. A hard fork is a change to the blockchain protocol which may cause a chain split where one version of the blockchain follows the new rules and the other follows the original rules.

[119] *See* Kyle Torpey, *BIP 9: Enabling Easier Changes and Upgrades to Bitcoin*, BITCOIN MAG. (Jan. 27, 2016), https://bitcoinmagazine.com/articles/bip-enabling-easier-changes-and-upgrades-to-bitcoin-1453929816 [https://perma.cc/JVM7-N7FZ].

[120] *See* Amy Castor, *How BIP 91 Enacts SegWit While Avoiding a Bitcoin Split*, COINDESK (Jan. 18, 2017), https://www.coindesk.com/coindesk-explainer-bitcoin-bip-91-implements-segwit-avoiding-split [https://perma.cc/GZG8-CKBG].

[121] JONES DAY, *supra* note 13, at 4.

c. Regarding the Users

Last but not least, collusive agreements may be implemented by certain blockchain users. In addition to the consensus mechanism that more or less facilitates agreements between miners and/or validators, on-chain governance mechanisms that allow users to make binding votes on network changes may support more coordination between miners and/or users.[122] More generally, depending on the consensus mechanism chosen by the blockchain, possession of a large part of the tokens may give power to impose decisions and/or coordination with other significant users. It should be remembered that 1,000 users own 40% of the Bitcoin market.[123] This problem also occurs on the Ethereum blockchain.[124] Generally speaking, supernodes are identified on the blockchain network. They are publicly visible to communicate and provide information to any other node that decides to establish a connection with them. They may, as a result, more easily come in contact with each other.[125]

B. Collusive Agreements Using Blockchain

Not all collusive agreements concern the conditions of access or use of the blockchain. Companies may also use blockchain to facilitate the creation and/or the functioning of collusive agreements about their strategies on the market, including prices, production levels, innovation strategies, and the like.

[122] Decred, Dfinity, and Tezos are working on putting such mechanisms on their respective blockchain. *See* WERBACH, *supra* note 5, at 217.

[123] *See* Olga Kharif, *The Bitcoin Whales: 1,000 People Who Own 40 Percent of the Market*, BLOOMBERG BUSINESSWEEK (Dec. 8, 2017), https://www.bloomberg.com/news/articles/2017-12-08/the-bitcoin-whales-1-000-people-who-own-40-percent-of-the-market [https://perma.cc/QL8M-JC9C].

[124] *See Thought Bitcoin Had a Whale Problem?*, *supra* note 110. It is partially solved by the fact that the more people use a blockchain, the less likely it is that one user or one mining pool will own 51% of the tokens. *See* Jon Matonis, *The Bitcoin Mining Arms Race: GHash.io and the 51% Issue*, COINDESK (July 17, 2014), https://www.coindesk.com/bitcoin-mining-detente-ghash-io-51-issue [https://perma.cc/5VZT-4TKH]. Also, on the whale problem resolution, see Crypto Li, *Bitmain Mining Pool Dominance Down 28% in H2 2018*, LONGHASH (Jan. 2, 2019), http://www.longhash.com/news/bitmain-mining-pool-dominance-down-28-in-h2-2018 [https://perma.cc/L2NR-SFR9] ("Antpool and BTC.com control 29% of total hashrate. This is down from over 41% in June. In just the last six months, Bitmain's mining pools have lost 28% of their market share, marking a shift toward greater decentralization of BTC mining. Many mining pools, even large ones, have a hard time holding on to their power.").

[125] *See* Sarah Finch*, At A Glance - Blockchain Supernodes*, DISRUPTION HUB (Oct. 29, 2018), https://disruptionhub.com/supernodes [https://perma.cc/2XHN-PA2J] (defining supernodes as highly connected points in a blockchain network, constantly running the blockchain software, but also, publicly connectable. Most blockchains require the holding of a certain number of tokens to qualify as supernodes.).

To date, how collusive agreements can be deployed on blockchain is a field that has yet to be explored. Here, I do so by making a distinction on whether or not the parties would use smart contracts. I also make a subdivision depending on whether the agreement would be taking place on a public or private blockchain.

1. Collusive Agreements Using Blockchain Without Smart Contracts

Consider the following example dealing with a collusive agreement using blockchain, but without a smart contract:

Three companies operating in the interior furniture distribution market want to agree on the origin of the raw materials they use to increase their negotiating power with their suppliers. For their cartel to be operational so that they can trust each other, they decide to refer to a public blockchain documenting the entire production chain of the products concerned. Based on this information, they meet every month in a restaurant and discuss the follow-up to their agreement.

Companies may choose to use a blockchain to enter into a collusive agreement.[126] The benefit they can find in this type of agreement over a non-blockchain agreement is the ability to ensure the visibility and traceability of the information that is shared. Depending on whether the blockchain is public or private, the blockchain offers different advantages.

When the blockchain is public, companies can ensure that they have access to all information that is listed in the same place, without any of the users being able to hide this information from others.[127] The blockchain also ensures that the information is certified. This reinforces the trust that users have in each other, and hence, the interest they may find in setting up such an agreement on a blockchain rather than outside it. Additionally, the public nature of the information can greatly complicate the task of antitrust and competition agencies wishing to qualify the agreement.[128]

[126] *See* Hitoshi Matsushima, *Blockchain Disables Real-World Governance*, at 3 (Univ. Tokyo, Ctr. for Research and Educ. for Policy Evaluation, Discussion Paper No. 55, 2019) ("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 designing a blockchain, see generally *Substrate*, PARITY, https://www.parity.io/substrate [https://perma.cc/2WMU-2SMG]. However, it can be assumed that the blockchain will be used for collusive agreements of a significant size rather than for agreements with little impact on the market.

[127] *See* Lin William Cong & Zhiguo He, Blockchain Disruption and Smart Contracts 20 (Oct. 6, 2017) (unpublished manuscript), https://ssrn.com/abstract=2985764 [https://perma.cc/JKL2-BCAN] ("greater information distribution may foster collusion which hurts competition").

[128] *See supra* Part II.

When the blockchain is private, all companies involved in a collusive agreement get exclusive and secure access to the information. This can help to strengthen cohesion between them. Private blockchain also allows the information to be certified before being integrated into its network, which, once again, creates a considerable advantage over physical or digital media other than blockchain.

2. Collusive Agreements Using Blockchain with Smart Contracts

Consider the following scenario helpful in understanding how blockchain can be used to prevent deviant behaviors:

Five companies create a cartel to divide the market between them. To make this agreement effective, they set up numerous smart contracts to ensure that colluders will comply with it. These companies choose to use a public blockchain that is accessible to all companies on the market. They use this information to create the most profitable agreement possible, and to ensure that none of the participants sell products in a territory that has not been allocated to them.

In this example, companies use blockchain combined with smart contracts to automate the agreement and to make the agreement more predictable and transparent. In the case of 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 automatically adjusted using different types of algorithms. For instance, a smart contract could automate transfers between the colluders and make side payments. Generally speaking, smart contracts may be used to execute any software, making contracts and collusions dynamic.[129] In the near future, smart contracts may also be used to integrate elements of artificial intelligence to detect the optimal balance of the agreement and act upon it.[130] Moreover, because these smart contracts are coded directly into the blockchain, it will not be possible to modify them without the agreement of the other users. This may strengthen the stability of the agreement.

In the case of a private blockchain, smart contracts may serve the same purpose as described for public blockchains — i.e., governing the relationship between users — and they may also be used to govern the framework of the agreement itself by deciding on the type of information published and who has access to it (which can be changed at

[129] For an explanation of how smart contracts may achieve that, see OPENLAW, https://openlaw.io [https://perma.cc/NMT3-ASPK]. Collusion using smart contracts is dynamic whereas collusion using only algorithms is static, as it cannot integrate software and external elements.

[130] *See* Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*, ALAMUT (Aug. 16, 1998, 10:37 AM), http://www.alamut.com/subj/economics/nick_szabo/smartContracts.html [https://perma.cc/GF5Y-3R3N] ("No use of artificial intelligence is implied.").

any moment in time). In other words, private blockchain allows the most sophisticated type of governance for implementing a collusive agreement using blockchain.

In both public and private blockchains, smart contracts can easily be implemented without technical knowledge.[131] Furthermore, they can be linked to one another through smart contract libraries, which may be used to supervise the interaction of different smart contracts.[132] Put differently, the execution of one smart contract could be conditioned to another one, and as such, proper blockchain governance of the collusion may be implemented.[133]

III. THE LIFE OF COLLUSIVE AGREEMENTS ON BLOCKCHAIN

Blockchain is an environment conducive to the quiet life of collusive agreements. In fact, collusion may "die" because of natural reasons (mainly due to changes in market conditions or the unstable nature of collusive agreements) or because a competition authority has detected the collusion.[134] Blockchain provides help on both fronts by preventing the colluders from cheating on the agreement and by reducing the detection risk.

In this Part, I combine the economic perspective of collusive agreements stability with the social perspective. For that, I study the "visibility effect" created by blockchain for the cartelist as well as the "opacity effect" created outside the collusive agreements. I then analyze to what extent this dual effect allows collusive agreements not to die because of natural reasons (deviance) or antitrust.[135] In short, I analyze how blockchain and smart contracts may be used to create and maintain order within collusive agreements. In this regard, when dealing with the question of punishments imposed by colluders on deviant companies, I focus on how sanctions may restore order while keeping the deviating member in, rather than excluding him permanently (for that, see Part IV).

[131] Multiple services offer to convert plain language into smart contracts. *See, e.g.*, OPENLAW, *supra* note 129.

[132] *See generally Contracts: Libraries*, SOLIDITY, https://solidity.readthedocs.io/en/develop/contracts.html#libraries [https://perma.cc/CVZ2-ZJY9].

[133] *See Interactions Between Smart Contracts with Solidity*, ZUPZUP, https://zupzup.org/smart-contract-interaction [https://perma.cc/XW9V-F89T] (detailing different ways to link smart contracts).

[134] Joseph E. Harrington, Jr. & Yanhao Wei, *What Can the Duration of Discovered Cartels Tell Us About the Duration of All Cartels?*, 127 ECON. J. 1977, 1979 (2016).

[135] Three situations are to be identified: "A cartel can then have three possible terminal states: (1) it can die a natural death (which we refer to as 'collapse') and not be discovered; (2) it can collapse and be discovered; and (3) it can be discovered (and thus die through conviction)." *Id.* at 1979–80.

A. The "Visibility Effect" for Colluders

Blockchain is a technology that can provide transparency. Colluders may monitor each other's market behavior more easily than outside of the technology. I label this the "visibility effect." Blockchain thus makes it possible, particularly through the use of smart contracts, to prevent deviant behaviors. In doing so, the technology ensures good cohesion to the agreement by strengthening the trust that colluders have in each other — or, at least, the trust they have in the information on which the collusion is based. The technology may also be used to correct deviant behaviors by imposing targeted sanctions. This is the "economic perspective" of cartel stability.

1. Blockchain as a Way to Prevent Deviant Behaviors

Consider the following scenario to understand how blockchain can be used to prevent deviant behaviors:

Five companies use a blockchain to inform their selling prices. These prices are automatically uploaded into the blockchain and smart contracts to monitor the company's prices. This makes the information visible to all colluders. Some of the members initially complained about this functioning because it makes it difficult to deviate from the collusive price, but all seem to have now understood that this allows the cartel to last longer.

Blockchain may be used to automate governance, and therefore, to prevent deviant behaviors. To understand why this is crucial to colluders, I must first analyze the conditions allowing for the sustainability of collusive agreements.

Collusive agreements tend to develop rapidly in markets where the effect of Porter's five forces greatly reduces overall profitability.[136] Profitability is generally reduced when there are high barriers to enter the market, poor substitutes, low bargaining power for buyers, low bargaining power for suppliers, and intense inter-firm rivalry. Stigler completes the analysis by underlining that cheating is less likely to be detected: "The larger the number of firms in the industry . . . [t]he more equal their sizes . . . [t]he more irregular the purchases of buyers . . . [t]he larger the buyers . . . [t]he less homogeneous the product, for price and quality are both elements of sales for a firm and quality is often difficult to measure."[137] Blockchain will help to create collusive agreements in these markets.

[136] ROBERT C. MARSHALL & LESLIE M. MARX, THE ECONOMICS OF COLLUSION: CARTELS AND BIDDING RINGS 23 (hardcover ed. 2012); Michael E. Porter, *How Competitive Forces-Shape Strategy*, HARV. BUS. REV., Mar.–Apr. 1979, at 137, 137.

[137] *See* GEORGE J. STIGLER, THE THEORY OF PRICE 226–27 (4th ed. 1987). *See also* Bolotova, *supra* note 56. ("Homogeneity of product and purchasing commitments, high market

It is also likely that blockchain will help colluders to maintain collusive agreements. Several elements explain the sustainability of explicit collusive agreements: (1) pricing structures allowing the implementation of a price increase, (2) allocation structures allowing cartel members to divide the collusive gain, and (3) enforcement structures facilitating the monitoring of deviant behavior.[138] The type of technical medium used to achieve the collusion can affect these three elements. Blockchain makes it possible, via smart contracts, to regulate the price operated by the colluders to find a balance point. Smart contracts can also allow an automatic division of earnings according to predefined criteria, and, of course, it makes it possible to monitor deviant behaviors[139] as well as to punish them, once again through smart contracts.

As for tacit collusive agreements, the Folk Theorem[140] is useful in studying the conditions under which companies find a collusive equilibrium without communication or transfers. Accordingly, when firms may observe each other's actions and interact with one another frequently, tacit collusion may occur and be stable. Public blockchains grant firms access to a large amount of information, and as such, the ability to observe other colluders' practices.[141] This will prevent deviant behaviors because the detection risk by other colluders is high. It is shown that collusion is stable when members have similar interests and can control other colluders' behavior[142] with mechanisms going beyond mere cheap talk.[143] Of course, the ability to detect cheating is not the only determinant of the cartel duration,[144] and accordingly, blockchain will not make cartels indefinite. Still, by easing the identification of deviant behaviors, collusive agreements become more stable.

This brings us back to the governance of collusive agreements. Empirical studies are irrefutable: the more sophisticated the governance,

concentration, small number of the sellers, inelastic demand, high barriers to entry, small size of the buyers, and availability of information are some of the factors that are likely to facilitate collusion.").

[138] MARSHALL & MARX, *supra* note 136, at 106–08. *See also* Christian Catalini & Catherine Tucker, *Antitrust and Costless Verification: An Optimistic and a Pessimistic View of the Implications of Blockchain Technology* (Mass. Inst. of Tech. Sloan, Research Paper No. 5523-18, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3199453 [https://perma.cc/Q6LS-HUS6].

[139] *See generally* Joseph E. Harrington, Jr., *How Do Cartels Operate?*, 2 FOUND. AND TRENDS IN MICROECONOMICS 1 (2006) (discussing importance of monitoring).

[140] Generally, the Folk Theorem refers to the fact that cooperative behavior can be sustained as an equilibrium in repeated games.

[141] Frédéric Marty, *Algorithmes de Prix, Intelligence Artificielle et Equilibres Collusifs*, 31 REVUE INTERNATIONALE DE DROIT ECONOMIQUE, 2017/2, at 83 (2017).

[142] Levenstein & Suslow, *supra* note 54, at 67, 69.

[143] KAPLOW, *supra* note 29, at 203.

[144] Although it is an important one. *See* D. K. Osborne, *Cartel Problems*, AM. ECON. REV., Dec. 1976, at 835, 835 (1976); *see also* PETIT, *supra* note 79, at 245.

the longer the collusion lasts.[145] About half of the collusive agreements die because of internal conflicts between their members;[146] these conflicts arise mainly after deviant behaviors. Blockchain will help colluders in this regard.[147] This technology allows for a greater sophistication of collusion by integrating algorithms and artificial intelligence[148] — in short, by automating governance. At the same time, the absence of human intervention will not be without some difficulties,[149] notably linked to the absence of flexibility in ex post decision-making.[150] For that reason, the way smart contracts are designed will impact the colluders' ability to adapt to market fluctuations, adaptation being also a determining factor in the life of collusive agreements.[151] In this sense, the colluders will have the duty to design smart "smart contracts."[152]

A path to insert some flexibility into the governance of collusive agreements using smart contracts would be to subject only part of the collusion to the blockchain, and part to legal contracts.[153] Such proceedings may prove to be attractive for parties wishing to avoid the limitation of smart contracts, which require the parties to choose between criteria that can be codified.[154] However, in doing so, the parties

[145] Levenstein & Suslow, *supra* note 54, at 71. *See also* Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, 100 AM. ECON. REV. 641, 650 (2010); Oliver E. Williamson, *Transaction-Cost Economics: The Governance of Contractual Relations*, 22 J.L. & ECON. 233, 235 (1979) (arguing that governance ensures "the integrity of a transaction").

[146] Levenstein & Suslow, *supra* note 54, at 75–76.

[147] *See* Cong & He, *supra* note 127, at 4.

[148] *See* KAPLOW, *supra* note 29, at 263 ("A greater difficulty is that sophisticated firms, aware of what inferences may be drawn from their price moves, may instead adjust prices strategically in order to disguise their coordinated behavior.").

[149] Notably, it removes smart contracts from the domain of judicial oversight, including mutual mistake, illegality, capacity, consideration, fraud, and duress. *See* WERBACH, *supra* note 5, at 126.

[150] Contracts, whether smart contracts or traditional contracts, are incomplete by nature as they do not cover all situations that may arise during their execution. Smart contracts, contrary to traditional ones, cannot be modified to accommodate a new situation.

[151] Successful collusion has produced organizational designs that allow the agreement to accommodate fluctuations in the external environment without requiring costly renegotiations. *See* Levenstein & Suslow, *supra* note 54, at 78.

[152] *See* WERBACH, *supra* note 5, at 163 ("Relying on smart contracts . . . [is] a bet on ex ante formalizations, which can never match the flexibility of ex post human decision-making.") For this reason, smart contracts do not resolve all conflicts and can even create some because they lack flexibility. Their design will therefore play a major role in the stability of the agreement.

[153] 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*, 33 BERKELEY TECH. L.J. 489, 544 (2018). Legal contract is here defined as a "program that runs on the brain of a lawyer." *See* Tim Ferriss, *Nick Szabo Interview | The Tim Ferriss Show (Podcast)*, YOUTUBE (Jun. 4, 2017), https://www.youtube.com/watch?v=3FA3UjA0igY [https://perma.cc/Y7Z5-72PY].

[154] WERBACH, *supra* note 5, at 125.

would lose the assurance of the proper execution of the agreement by de-automating part of it.

In short, blockchain creates a means to monitor colluders more closely. This effect can only be mitigated by two elements. First, the blockchain may be private and designed in such a way that not all users have access to all transactions on it. In this case, only the creator of the blockchain and some designated users will have access to it in its entirety. This reduces the visibility for all users and at the same time reinforces the role of the blockchain creator as a leader. Second, although transactions recorded in the blockchain are visible to all users, they may not have access to the specifics of each transaction (such as price and quantity sold).[155]

Despite these two limits, blockchain drastically increases colluders' ability to monitor each other in comparison to what can be done outside the blockchain. First, if one of the colluders deviates from the collusive price, an increase of the deviant's sales will appear on the blockchain. Furthermore, when companies use smart contracts, rule-making and rule enforcement are made possible at the same time,[156] which reinforces the trust colluders have in the agreement. For these two reasons, the visibility of other colluders' behavior remains greater on the blockchain than off it.

2. Blockchain as a Way to Correct Deviant Behaviors

Consider the following example showing how blockchain can be used as a way to correct deviant behaviors:

Four companies want to create a cartel using blockchain and to make it last long enough so the risk they take is worth it. For that, they require that each colluder initially sends ten tokens into the blockchain. The colluders are entrusted to a smart contract, making the contract the central point of the management of the blockchain. These tokens are redistributed depending on the behavior of each colluder. It encourages colluders not to engage in deviant behaviors. Using smart contracts, the mechanism forces deviant colluders to pour more tokens into the common pot. The punishment imposed thus compensates for the damage caused by the deviance.

Here, I analyze which type of punishment can be put in place to restore stability without ejecting any member from the agreement. In

[155] This is not true for private blockchains. *See* YAGA ET AL., *supra* note 13, at 5.

[156] *See* Vili Lehdonvirta, *The Blockchain Paradox: Why Distributed Ledger Technologies May Do Little to Transform the Economy*, OXFORD INTERNET INST. (Nov. 21, 2016), https://www.oii.ox.ac.uk/blog/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy [https://perma.cc/6UZ7-J9BZ]. Indeed, "both the specification of rights and obligations and the execution of that contractual agreement occur through the platform." *See* WERBACH, supra note 5, at 64.

other words, I consider how smart contracts can may correct deviant behaviors.

A historical study of collusive agreements tends to show that collusion survives most deviant behaviors as long as deviations do not question the pricing structure.[157] Smart contracts will seek to correct such deviance by putting in place automated and targeted punishments. "[O]ne of the greatest curbs on crime is not the cruelty of punishments, but their infallibility . . . The certainty of punishment even if moderate will always make a stronger impression."[158]

As far as intentional deviant behaviors are concerned,[159] colluders must impose an effective and visible sanction.[160] The threat of a return to a competitive situation may deter such behavior,[161] but ideally, the punishment must be directed only at the deviating member.[162] Blockchain can be helpful in doing so, for instance, by automatically changing the costs incurred to participate in the collusion. One way is to request an initial payment of tokens to participate in the agreement and then automatically regulate their distribution based on compliance with the agreement.[163] More simply, the participation fees in the blockchain can be regulated according to the behavior of each colluder, making it more expensive for certain members to be part of and/or deviate from the agreement.

Unintentional deviant behaviors are usually not problematic, as long as their number is limited and as long as deviations can be compensated in a way to preserve each colluder's self-interest. In this regard, blockchain and smart contracts make it possible, when necessary, to correct deviant behaviors by ensuring a fair balance through a redistribution of the extra profits made by the deviant member between all colluders. As such, blockchain and smart contracts improve the stability of collusive agreements.

Whether the deviation is intentional or not, smart contracts should compensate for the gains made by a deviating member to avoid any lucrative infringement (which occurs when the gains are higher than the punishment). This economic perspective of cartel stability depends on the perceived and actual profits that result from cheating compared to

[157] MARSHALL & MARX, *supra* note 136, at 106.

[158] BECCARIA, *supra* note 1, at 58.

[159] Of course, intentional deviation is still possible despite the blockchain because "[m]achines may be running the code, but humans are acting on it." WERBACH, *supra* note 5, at 109.

[160] *See* Daniel Orr & Paul W. MacAvoy, *Price Strategies to Promote Cartel Stability*, 32 ECONOMICA 186, 186 (1965).

[161] MARSHALL & MARX, *supra* note 136, at 136. *See also* Ian Ayres, *How Cartels Punish: A Structural Theory of Self-Enforcing Collusion*, 87 COLUM. L. REV. 295, 302 (1987).

[162] MARSHALL & MARX, *supra* note 136, at 137.

[163] *See* Vitalik Buterin, *Decentralizing Everything*, YOUTUBE (Sept. 18, 2017), https://www.youtube.com/watch?v=WSN5BaCzsbo [https://perma.cc/4Q5K-TLH2] (discussing this mechanism).

the likelihood of possible punishment by other colluders.[164] Blockchain, by increasing the detection of deviant behaviors and the potential accuracy of punishments, will raise the costs of misbehaving and will make collusive agreements more stable. After all, "[a] smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[165] Smart contracts make it easier for parties to keep their word.

B. The "Opacity Effect" for Outsiders (Including Agencies)

Despite the creation of a strong "visibility effect," blockchain creates a concomitant "opacity effect." Blockchain allows for greater transparency but also ensures the secrecy of certain information. In doing so, blockchain strengthens members' trust in each other because it protects them from detection by antitrust and competition agencies. Blockchain also strengthens the members' mutual trust because it greatly complicates agencies' investigations into the collusive agreements that have come under their consideration. This is the "social perspective" of collusive agreements' stability.

1. Blockchain as a Way to Protect Colluders from Detection

As I have shown, public and private blockchains provide users with different opacity settings. Public blockchains are freely accessible, and all information contained in them is part of the public domain, insofar as anyone can access it without even "entering" the blockchain.[166] No membership or authorization is needed, and the information is available to everyone at any given time. For example, the history of all transactions made using Bitcoin is available to all, whether people are Bitcoin owners or not.

Private blockchains, in this regard, have opposite features. Information stored on private blockchains is only available to their users and can only be channeled to some users.[167] In the case of collusion, the ringleader may choose to create a hub and spoke in which only he can access all information and manage the collusion.[168] Alternatively, he

[164] J. D. Jaspers, *Managing Cartels: How Cartel Participants Create Stability in the Absence of Law*, 23 EUR. J. ON CRIM. POLICY & RES. 319, 321–22 (2017) ("[C]artels invest more in means to prevent cheating than to resort to ex post punishments, which are costly.").

[165] Szabo, *supra* note 130.

[166] *See* YAGA ET AL., *supra* note 13, at 44.

[167] *See* WERBACH, *supra* note 5, at 62, 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.").

[168] *See* Catalini & Tucker, *supra* note 138, at 4; *see also* JONES DAY, *supra* note 13, at 2.

may choose to give access to all users of the private blockchain. By doing so, it is expected that users will monitor each other.[169]

The difference between the two types of blockchains in terms of opacity and access to their information has a great impact on collusive agreements' durability. I have shown that the "visibility effect" — the fact that companies can monitor each other on public blockchains and most private blockchains — helps to police deviant behaviors. But there is more. Information is made more visible for colluders when the agreement uses blockchain than when it does not, but in parallel, the same information is made less visible for non-colluders, such as competitors and agencies. Blockchain then generates a "visibility effect" (among colluders), while at the same time generating an "opacity effect" (among non-colluders). This effect exists on public blockchain because all transactions are being hashed through the blockchain cryptographic function[170] and because the identities of blockchain users are protected by pseudonymity.[171] It is even stronger in the case of private blockchains because their existence may be kept secret, entry to them made impossible to intruders, and the reading of the blocks and transactions limited to the authorized users.

The opacity effect protects colluders from detection by antitrust and competition authorities. When the fear of detection is partially or entirely dispelled, it reinforces the mutual trust that colluders have in each other. This is a key element of collusion longevity as it has been shown that "a rise in the probability of detection and conviction [] causes the immediate collapse of the least stable cartels."[172] Antitrust and competition agencies seek to maximize distrust, but when companies use blockchain, it becomes harder to create an incentive to defect. Stable collusion in which members trust each other is better for them than stopping the practice and applying for leniency. In other words, lowering the probability of detection encourages colluders to maintain their participation.[173] This is precisely the "social perspective" of the stability of collusive agreements.[174]

[169] Generally, such cartels tend to fail rapidly. *See* Joseph E. Harrington Jr, How Do Hub-and-Spoke Cartels Operate? Lessons from Nine Case Studies 4 (Aug. 24, 2018) (unpublished manuscript), https://ssrn.com/abstract=3238244 [https://perma.cc/N7PV-EXQ9].

[170] *See* WERBACH, *supra* note 5, 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.

[171] *See* Schrepel, *supra* note 57, at 309.

[172] JOSEPH E. HARRINGTON JR., THE THEORY OF COLLUSION AND COMPETITION POLICY 27 (2017).

[173] *See* Jaspers, *supra* note 164, at 332; Oindrila De, *Analysis of Cartel Duration: Evidence from EC Prosecuted Cartels*, 17 INT'L J. ECON. BUS. 33, 38 (2010).

[174] Jaspers, *supra* note 164, at 322–24.

"Death by antitrust" and the risk of detection by antitrust and competition agencies are not the only causes of the death of collusions. Leniency procedures and complaints from outside the agreement are two major causes as well. And yet, empirical studies tend to show that collusive agreements are live shorter when competition authorities expand enforcement efforts towards detecting them.[175] The less stable the collusive agreement, the more likely it is to collapse if an agency focuses its best efforts on this issue.[176] Differently put, the detection risk has a direct impact on the stability of all collusive agreements. This is only true, however, if the collusion can be detected in the first place. By technically protecting the colluders, blockchain could very well reverse the situation. The overall level of stability could therefore be increased, as it is understood that some collusive agreements, depending on their governance, would be more stable than others.

Finally, this opacity effect will also have an impact on the type of agreements. The increase in colluders' trust, thanks to blockchain, will lead to more aggressive collusion. If the detection risk is high, colluders should in their best interests only set up an agreement that deviates slightly from the competitive price.[177] But where the detection risk is low, the colluders generally deviate substantially from the competitive price.

2. Blockchain as a Complication to Agencies' Investigations

The opacity effect does not entirely prevent antitrust and competition agencies from detecting collusion. Two methods are used to detect such agreements: one reactive and decentralized, the other proactive (ex officio) and centralized.[178] The first mainly utilizes complaints, whistleblowers, grand juries, informants, search warrants, dawn raids, and leniency applicants, which blockchain cannot prevent.[179] However, blockchain can greatly complicate this method in several ways, which are explained in Part IV of this Article. The second results from market surveillance, industry monitoring, and screening, since collusion effects may appear outside of the medium (here, the blockchain).[180] In short, such proactive methods aim to identify anti-competitive effects

[175] *See, e.g.*, Margaret C. Levenstein & Valerie Y. Suslow, *Breaking Up Is Hard to Do: Determinants of Cartel Duration,* 54 J.L. & ECON. 455 (2011).

[176] Harrington & Chang, *supra* note 44, at 1401–02.

[177] George J. Stigler, *A Theory of Oligopoly*, 72 J. POL. ECON. 44, 46 (1964).

[178] PETIT, *supra* note 79, at 693; *see also* Org. for Econ. Co-operation and Dev. [OECD], *Ex Officio Cartel Investigations and the Use of Screens to Detect Cartels*, at 87–88, DAF/COMP(2013)27 (Jul. 7, 2014).

[179] *Ex Officio Cartel Investigations*, *supra* note 178, at 92–93.

[180] Defined as "[t]he ability to flag unlawful behavior through economic and statistical analyses." *See* Rosa M. Abrantes-Metz, Proactive vs. Reactive Anti-Cartel Policy: The Role of Empirical Screens 2 (June 2013) (unpublished manuscript), https://ssrn.com/abstract=2284740 [https://perma.cc/44YC-K83K].

visible outside of the blockchain to find the real-life identity of the suspect, infiltrate the computer to recover the private key, and make the link between the public key and identity.

There are two general types of approaches to the proactive detection of collusive agreements: one structural and the other behavioral.[181] The structural approach involves the screening of certain markets in an attempt to identify collusive agreements. Typically, an antitrust authority decides on an industry to screen and determines whether it exhibits characteristics that make the firms inclined to collude. The behavioral approach is designed to flag firms' behaviors or market outcomes to detect any patterns of collusive agreements.[182] Both types eventually rely on market-based evidence, and mainly, pricing patterns.[183] Considering that, in the words of Richard Posner, "[e]conomically significant collusion should leave some visible traces," blockchain does not help companies in this regard because effective collusion will remain visible.[184]

Blockchain will nevertheless help companies regarding the other factors analyzed by authorities before studying the pricing patterns. The first of these factors is the conduciveness of conditions,[185] including the number of companies and market concentration, the firms' capacities, the transparency of prices and the structure of the buyer side of the market, product heterogeneity, the similarity of colluders, and the industry elasticity of demand.[186] These conditions are useful to authorities in determining which markets to screen. Blockchain will make this first factor more ambiguous as real identities are not displayed and the nature of transactions is kept secret. The second factor relates to internal evidence.[187] Entering into a collusive agreement generates all sorts of documents that explain why an agreement was formed. When coupled with smart contracts, blockchain automates many aspects of collusive agreements and then removes some of this internal evidence. The third factor for detection outside of market-based evidence is inter-firm communication.[188] The actual ability to study such a factor is limited, and the use of this factor becomes harder, as inter-firm contacts are confined to a few individuals, and are more confidential due to the use of private

[181] *Ex Officio Cartel Investigations*, *supra* note 178, at 20.

[182] Joseph E. Harrington, Jr., *Detecting Cartels*, *in* HANDBOOK OF ANTITRUST ECONOMICS 213, 213 (Paolo Buccirossi ed., 2008).

[183] KAPLOW, *supra* note 29, at 259 ("Certain pricing patterns may indicate successful oligopolistic coordination or a breakdown that implies its prior existence."). For a list of these patterns, see *Ex Officio Cartel Investigations*, *supra* note 178, at 28.

[184] Richard A. Posner, *Oligopoly and the Antitrust Laws: A Suggested Approach*, 21 STAN. L. REV. 1562, 1587 (1968).

[185] *See* KAPLOW, *supra* note 29, at 286.

[186] *See id*. at 289–91.

[187] *See id*. at 295.

[188] *See id*. at 302.

blockchains. In the end, blockchain largely complicates the work of authorities, and it seems, for the aforementioned reasons, that authorities will have to find market-based evidence in a more random way than they do now.

On top of that, while prices to end consumers are public, this is generally not the case for prices between companies. Blockchain will make it even harder to access them, and generally, to identify the chain of B2B transactions which may go through different blockchains through the process of production, for instance. One must add that even once detected, blockchain will complicate the investigation of companies involved in B2B or B2C collusion for technical reasons. For instance, only the users in private blockchains that are the intended recipients of the data can access and read the block of information, which greatly limits agencies' ability to gather evidence. Furthermore, antitrust and competition agencies will not be able to rely too much on the use of algorithms to detect and document collusive agreements.[189] We have seen that blockchain is indeed a fortress[190] — immutable and pseudonymous. Blockchain will therefore prevent the collection of useful information, a point that is often overlooked when tech-optimists describe the new tools available to authorities.[191]

Overall, the help provided by blockchain in ensuring the stability of collusive agreements is beneficial to colluders and, not surprisingly, detrimental to antitrust and competition authorities. This help is also greatly problematic for parent companies, who may be prevented from detecting collusive practices by their subsidiaries. This could create a problem when deciding whom to fine. Admittedly, there is no presumption of accountability in private enforcement, but such a presumption exists in public enforcement. The following question then arises: should this presumption be maintained in the blockchain context? In the meantime, it will be up to parent companies to ensure a proper flow of information regarding the actions of their subsidiaries.

In short, mostly for technical reasons, blockchain greatly complicates the work of antitrust and competition agencies. Detecting first anti-competitive practices on blockchain and then tracing back to the private key is highly complicated by the technology. Only the other way around is possible; going from the practice to the proof on blockchain. It is now up to these agencies to increase their understanding of the technology to be able to analyze them when it is necessary. In the

[189] *See* Michal Gal, *Algorithms as Illegal Agreements*, 34 BERKELEY TECH. L.J. 67, 115 (2019).

[190] *See* Schrepel, *supra* note 57, at 322–23.

[191] *See* Org. for Econ. Co-operation and Dev. [OECD], *Summary of Discussion of the Roundtable on Algorithms and Collusion*, at 2, DAF/COMP/M(2017)1/ANN2/FINAL (Sept. 26, 2018) (discussing the use of algorithms by antitrust and competition agencies).

absence of such substantive work, their investigations will be complicated by the coding of contents of a transaction, the protection of users' identity, and the use of smart contracts. Extensive technical knowledge of blockchain is now required for agencies if they want to maintain their regulatory ability.

IV. THE DEATH OF COLLUSIVE AGREEMENTS ON BLOCKCHAIN

Blockchain is an environment — an ecosystem, some would say — that is conducive to the death and disappearance of collusive agreements. Smart contracts may indeed be used to automate the exit from collusion. In that sense, the technology strengthens the cohesion of colluders until the dissolution, which will be accelerated and better coordinated. For this reason, the number of leniency applications may very well decrease. If companies can indeed organize their exit from collusion, and even more, the conditions of their exit, it will lead to shorter periods of hesitancy as to whether they should maintain their participation in the agreement and less post-collusion dissatisfaction.

A. The Use of Smart Contracts to Exit Collusive Agreements

Smart contracts may be used to exit collusive agreements, whether it is to force the exclusion of a deviant colluder or for a company to manage its own exit from the agreement. These automated exits might be organized in accordance with several pre-established rules, ultimately leading to new challenges for antitrust and competition agencies.

1. Smart Contracts as a Way to Force the Exclusion of a Deviant Colluder

Consider the following scenario, helpful in understanding how blockchain can be used to force the exclusion of a deviant colluder:

Five companies collude regarding their prices in the food distribution sector. Several smart contracts automate transactions, so each sale made by one of these distributors is registered into the blockchain.[192] *This mechanism makes it possible to monitor the agreement and thus to discourage deviant behavior.*

[192] *See* Evan Schwartz & Stefan Thomas, *Smart Oracles: A Simple, Powerful Approach to Smart Contracts*, GITHUB (July 17, 2014), https://github.com/codius/codius-wiki/wiki/White-Paper [https://perma.cc/Q9SR-MM8C] (using "oracles" which are connecting smart contracts with "real world" data).

The members of the collusion discuss the conditions under which a behavior will be considered deviant and will thus be punished. One option is that if one of these companies sells its products 20% cheaper than the collusive price for a period of more than a week, it will automatically be ejected from the blockchain. This mechanism would be known by all the colluders and would strengthen their willingness to comply with the agreement. The second option is less severe. The conditions for considering a member to be deviant are the same, but the deviant colluder would be deprived of access to the entire blockchain. His fees to register transactions would also be made automatically higher, so his overall participation is made slightly less profitable. This would encourage him to join the ranks.

Here, I no longer discuss the punishments that can be put in place to restore the stability of the agreement, but those that can lead to the exclusion of a deviant colluder. As far as public blockchains are concerned, none of the colluders have the actual power to exclude another user from the blockchain. Plus, talking about the exclusion from such blockchains is nonsensical since there is no formal entry — again, they are accessible to all, at any given time. As far as private blockchains are concerned, the exclusion may be total or partial as it is possible to modulate the three degrees of blockchain use: reading the information, adding transactions, and validating the blocks. This type of blockchain therefore offers many possibilities of exclusion other than those of smart contracts. With this power of exclusion comes a greater risk for the companies involved. They may be guilty of monopolization or abuses of dominance in this regard.[193]

Regardless of the type of blockchain used, empirical evidence suggests that collusion stability is put in danger when sanctions are effectively imposed. Collusion in which a deviating member has been sanctioned is less stable than others.[194] That is why collusive agreements invest more in detection tools, which help in preventing deviation and maintaining the agreement, than in the sanctions themselves.[195] In fact, one of these tools could be the blockchain itself. Consider a situation in which blockchain is used as a court system to resolve disputes securely. In such a case, the blockchain is only used in specific scenarios where there is a disagreement between users. For instance, if one of the users challenges the validity of a transaction, a mechanism

[193] *See* Thibault Schrepel, *Predatory Innovation: The Definite Need for Legal Recognition*, 21 SMU SCI. & TECH. L. REV 19, 21 (2018) (noting that companies may be sanctioned for having implemented predatory innovations).

[194] *See* Levenstein & Suslow, *supra* note 175, at 455.

[195] *See* Jaspers, *supra* note 164, at 322 ("[C]artels invest more in means to prevent cheating than to resort to ex post punishments, which are costly.")

may be activated to submit the transaction to the blockchain for verification. All other uncontested transactions would not be submitted to the blockchain, which could solve the scalability issue.

In short, the main challenge for collusive agreements that take place on the blockchain will be to find a fair balance between the implementation of smart contracts that make it possible to dissuade deviant behaviors (and, thus, to manage collusive agreements) and the desire not to introduce too strict or too regular punishments. After all, once one member is ejected from the collusion, the entire agreement could be destabilized.

2. Smart Contracts as a Way to Manage a Company's Own Exit from the Collusion

Consider now the following example showing how smart contracts could be used by a company to exit a collusion:

Three companies have decided to create a cartel and to use a blockchain as the medium to facilitate it. Several smart contracts govern their relationships, some of which are specifically designed to be ejection seats. One of the smart contracts allows companies to leave the blockchain when deviant behavior is observed for more than a week. Another smart contract allows the same automatic ejection from the cartel when one of the participants increases its sales by more than 30% over a comparable period, assuming that such an increase signals a deviant behavior on prices that are not documented on the blockchain. Another smart contract can be activated at will by colluders while permitting the destruction of the data published on the private blockchain. This aims to complicate (if not to prevent) the characterization of an agreement or even a concerted practice for antitrust and competition agencies.

Smart contracts can be used by the parties to enable them to exit collusive agreements, whether this is automatic or on-demand. As far as public blockchains are concerned, the identity of blockchain users is protected by pseudonymity.[196] Even if each colluder knows the real-life identities of other colluders, it will be difficult for antitrust and competition agencies to use such evidence unless they carry out a dawn raid to establish the link between the blockchain identity and the one in real

[196] *See* WERBACH, *supra* note 5, at 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."). It shows that there is a race. It is uncertain which of the developers or these tracking companies will win it. Ethereum, which is working on incorporating quantum resistance into its design, shows that the barriers created by blockchain are getting thicker. Furthermore, for now, these tracking services work with blockchains using 'not so strong' designed architectures. The supposed non-existence of pseudonymity must therefore be largely put into perspective. On that, see Schrepel, *supra* note 57, at 322–23.

life. Moreover, although the destruction of evidence seems impossible on this type of blockchain, insofar as it will lead to the sole creation of a fork, this drawback for colluders is compensated by the absence of governance on blockchain, making it more difficult for the antitrust and competition agencies to conduct their investigations.[197] With a more social perspective, one could still argue that potential colluders will be discouraged from using the blockchain for illegal purposes. It will be interesting in this regard to monitor the sociology of blockchain uses in the coming years. It remains likely that blockchain will be used for illegal purposes because colluders do not necessarily think about the risk of detection when entering into a collusive agreement.[198]

Private blockchains may allow an on-demand exit from the agreement while ensuring the deletion of data.[199] This is highly attractive for potential colluders to the extent that they can destroy evidence outside the blockchain while still enjoying the benefits of the technology. More generally, considering the fact that the owner of a private blockchain retains the right to override, edit, and delete the entries on the blockchain,[200] or even to modify the functioning of the blockchain itself,[201] the blockchain cannot be used as tangible evidence to prove participation in collusion.[202] This is in contrast to public blockchains. The identity of private blockchain users is more easily associated with real-life identity, not because of technical reasons, but because the creator of the blockchain has selected them, potentially based on their real-life identity. It may therefore be possible, to some extent, to ask the blockchain creator to communicate these identities. Nonetheless, by allowing the parties to delete their data and transactions, colluders may remain safe from detection. Only a copy of the data held by another colluder could potentially put the colluders into great danger.

[197] *See* Peder Østbye, The Case for a 21 Million Bitcoin Conspiracy 11 (Mar. 8, 2018) (unpublished manuscript), https://ssrn.com/abstract=3136044 [https://perma.cc/VAN3-GAW9] (arguing that for "cryptocurrencies where the operators are pseudo-anonymously spread over a manifold of jurisdictions, enforcement is impractical").

[198] *See* Ulrike Malmendier & Timothy Taylor, *On the Verges of Overconfidence*, 29 J. ECON. PERSP. 3, 3 (2015) (explaining that this is because humans, including cartelists, are over-confident).

[199] Indeed, immutability is easier to undermine on a blockchain if all the participants decide to do so together. Smart contracts, agreed upon by the blockchain users, may then do so for each of these users.

[200] *See* Catalini & Tucker, *supra* note 138, at 11 ("[P]ermissioned blockchains are not necessarily immutable, and key participants could technically collude to rewrite the log of transactions before discovery takes place."); *see also* YAGA ET AL., *supra* note 13, 34 ("For permissionless blockchain networks, the adoption of a longer, alternate chain of blocks could be the result of a form of attack known as a 51% attack."). For an explanation of the hard fork made by Ethereum, *see* Yeung, *supra* note 84, at 234.

[201] *See* S. U. Breu, *Are Blockchains and Cybercurrencies Demanding a New Legislative Framework*, 1 J.L. & DIGITAL ECON. 12, 13 (2018) ("In contrast to the public blockchains, consortium or private blockchains can easily change rules and entries in the ledger and even revert processes.").

[202] *See* JONES DAY, *supra* note 13, at 3.

In the end, smart contracts can be used to accelerate the dissolution of collusive agreements, or at least, of collusion that is faltering. This is the case when colluders suspect that an antitrust or competition authority may detect them (causing "death by antitrust"), or quite simply when there is a strong disagreement between them (causing a "natural death," which the blockchain alone cannot prevent). Thus, by facilitating the identification of deviant behaviors, blockchain is not only a means of solidifying collusion, but also of weakening it.

B. Smart Contracts vs. Leniency Applications

Blockchain, coupled with the use of smart contracts, may cause a decrease in the number of leniency applications. This is not necessarily problematic. After all, both smart contracts and leniency procedures contribute to the cessation of illegal practices.

1. The Impact of Blockchain on Leniency Applications

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

The first element concerns the current trends in leniency applications in both Europe and in the United States. In Europe, the number of applications fell by half between 2014 and 2016.[203] The same can be observed in the United States.[204] It shows unequivocally that the leniency procedure is facing difficult days. The arrival of the blockchain will not make things any easier.

The second concerns the technical difficulties created by blockchain. The technology is indeed creating a fortress that greatly complicates the work of antitrust and competition agencies.[205] Firstly, it protects the identity of users, which is all the more true in the context of a public blockchain where there is no need for users to be approved by the creator of a blockchain. Secondly, the transactions that are recorded on the blockchain are encoded and cannot be decrypted by a party other than those in the transaction. This also protects colluders by not allowing agencies to trace collusion history. Thirdly, even if the identities of the users were known by obtaining users' private keys and even

[203] *See* Johan Ysewyn & Siobhan Kahmann, *The Decline and Fall of the Leniency Programme in Europe*, 1 COMP. L. REV. 44, 45 (2018) ("In 2014 there were 46 leniency applications, which dropped to 32 applications in 2015, and finally only 24 applications have been registered in 2016.").

[204] *See* Charles McConnell, *Type A Leniency Applications Down, US DOJ Official Says*, GLOBAL COMPETITION REV. (June 15, 2018), https://globalcompetitionreview.com/article/1170614/type-a-leniency-applications-down-us-doj-official-says [https://perma.cc/88UH-XEZA].

[205] *See* Schrepel, *supra* note 57.

if the purpose of the transaction was also known, it would be very difficult, if not impossible, depending on the type of blockchain, to impose the deletion of the data contained therein.[206] The anti-competitive nature of some information could therefore benefit companies on the market, even after the collusive agreement has been detected by an agency. In this respect, it could even be argued that the exit of companies with the automatic destruction of information by smart contracts would be preferable to a leniency application without any subsequent possibility of eliminating the collusive agreement.

The third element is linked to the fact that, in addition to its technical characteristics, blockchain makes it possible to manage the risk of detection, which will logically reduce the number of leniency applications. Indeed, in the case of public blockchains, the parties may agree to use only data accessible by all companies while secretly ensuring that smart contracts automatically correct market anomalies caused by the collusion. The public nature of the information, coupled with smart contracts that adjust the terms of the agreement, will build greater trust between colluders.[207] Private blockchains can be set up in a way that not all users have access to the entire blockchain. This greatly reduces the risk of one colluder applying for leniency, considering the fact that applicants are required to hand over evidence to the antitrust authority. By depriving some users of access to all the information on the blockchain, it will be difficult for the users to negotiate full immunity or even second rank leniency to the extent that they may not be able to provide sufficient information to agencies.

As a consequence, blockchain may very well become the principal means for the end of collusion when the colluders fear detection, rather than leniency applications. The higher the risk of detection, the more participants will be forced to position themselves and choose between leniency and an exit through smart contract.[208] The technical difficulties created by blockchain with regard to agencies' possible investigations will also be taken into account by colluders.[209] At the very least, blockchain will give them enough security not to rush into a leniency application. As such, there is every reason to believe that blockchain will soon overshadow leniency applications, at least partially.

[206] Once again, immutability is easier to undermine on such blockchain if all the participants decide to do so together. Smart contracts, agreed upon by the blockchain users, may then do so for each of these users.

[207] J. David Lewis & Andrew Weigert, *Trust as a Social Reality*, 63 SOC. FORCES 967, 976 (1985) ("Trust begins where prediction ends.").

[208] Evgenia Motchenkova, *Effects of Leniency Programs on Cartel Stability*, at 1 (Tilburg Univ. Center Discussion Paper, No. 2004-98, 2004).

[209] *See* Saller, *supra* note 43, at 14 (stating that a high risk of detection is a prerequisite for an effective leniency programme).

At first sight, the expected decrease in the number of leniency applications may seem particularly problematic as antitrust and competition agencies are increasingly relying on them to detect collusive agreements.[210] According to the OECD:

> The percentage of cartel cases detected through leniency applications is reported in the survey to range between 45–55% for countries like Canada, Chile, Germany, Korea, and New Zealand and up to 80% for the EU (OECD, 2017). In the US, over 90% of penalties imposed by the US Department of Justice (DOJ) were linked to investigations assisted by leniency applicants.[211]

This shows a very reactive policy on the part of antitrust and competition agencies. This also sends a signal to companies: a well-designed collusive agreement that frames and rectifies disagreements has a good chance of (long) survival.[212]

By undermining the effectiveness of leniency, blockchain will force competition agencies to become proactive again to readjust the balance, failing which companies will have a growing sense of immunity from antitrust and competition law. In addition, strengthening proactive detection will increase the risk of punishment, and thus will force companies to seek leniency again.[213] It is a true virtual circle. I therefore recommend that agencies focus their best efforts in this direction by engaging in market surveillance, industry monitoring, and screening,[214] while keeping in mind that their detection work will be complicated by the opacity effect created by blockchain.[215] But the screening of collusive agreements remains possible on certain aspects, notably on

[210] *Id.* at 22; *see also Ex Officio Cartel Investigations*, *supra* note 178, at 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.").

[211] Saller, *supra* note 43, at 4; *see also* European Parliament, Answer to Parliamentary Questions E-0890/09, E-0891/09, & E-0892/09 (Apr. 2, 2009) (stating that in Europe, forty-six out of fifty-two cartel decisions (88%) from 2002 through 2008 were triggered by a leniency application).

[212] *See* Hans Wolfgang Friederiszick & Frank P. Maier-Rigaud, *Triggering Inspections* Ex Officio*: Moving Beyond a Passive EU Cartel Policy*, 4 J. COMPETITION L. & ECON. 89 (2008). Levenstein & Suslow, *supra* note 54, at 71.

[213] *See id.* at 5.

[214] *But see id.* at 214 ("At this time, the DOJ has no plans to redeploy investigative resources into screening for indications of cartel activity. The DOJ has had continuing success with the many other means for generating investigative leads.").

[215] *See supra* Section III.B.

market behaviors, which must be put at the center of antitrust and competition agencies' attention. It implies, again, that authorities first develop expertise on the subject of blockchain, a prerequisite for an effective proactive policy.

2. Smart Contracts and Leniency: A Similar End

In its *Notice on Immunity from fines and reduction of fines in cartel cases*, the European Commission made it clear that leniency programs exist to detect illegal collusive agreements and to stop them.[216] The European Commission stresses that "by their very nature, secret collusive agreements are often difficult to detect and investigate," holding that as a consequence rewarding undertakings willing to put an end to their participation is in the Community's best interest.[217] As I have shown, the same view is shared in the United States, where leniency programs are seen as a "prompt and effective" means to stop companies from further participation in collusive agreements.[218]

Smart contracts can achieve the same end. The creation of collusion using blockchain will not eliminate all leniency applications, but by discouraging deviant behaviors, by automating punishments, and by giving means to exit the agreement under predetermined conditions, it is expected that the number of leniency applications will drop.[219] This is not necessarily as problematic as it seems, as the amount of "natural" deaths of collusive agreements using blockchain is expected to be higher than it is today. The decrease in the number of "deaths by antitrust" will then probably be compensated.

Moreover, deaths by antitrust do not entirely purge the detection risk. Public blockchain could potentially remain there as proof of past practices, although antitrust authorities will be faced with the difficulty of identifying users.[220] The same antitrust authorities will not necessarily be able to identify which transactions are the result of smart contracts on the blockchain. It will always remain possible for authorities,

[216] In theory, the leniency application is only open to horizontal cartels and leaves out the exchange of information. *Commission Notice on Immunity from Fines and Reduction of Fines in Cartel Cases*, 2006 O.J. (C 298) 11.

[217] *Id.* at 17.

[218] *See* U.S. DEP'T OF JUSTICE, ANTITRUST DIV., FREQUENTLY ASKED QUESTIONS ABOUT THE ANTITRUST DIVISION'S LENIENCY PROGRAM AND MODEL LENIENCY LETTERS 4 (2017), https://www.justice.gov/atr/page/file/926521/download [https://perma.cc/C2K3-7UNB].

[219] 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*, 30 WORLD COMPETITION L. & ECON. REV. 25 (2007).

[220] *See* WERBACH, *supra* note 5, at 129 (stating that most digital wallets are a point of failure. Users must trust their provider "in the same manner as with a bank. The wallet provider stores the private cryptographic key.").

however, to carry out dawn raids to seize computers and try to identify the colluders and their practices. In the case of a private blockchain, only the blockchain creator(s) will have the capacity to grant access to antitrust and competition agencies. One could imagine that this power will be used to blackmail colluders and former members. This is one of the major consequences created by the natural death of collusive agreements instead of death by antitrust.

Purging the risk that authorities will detect the collusion after the colluders have left the blockchain is, however, possible. It could be done, first, if all the colluders agree to do so. They could indeed create a soft or a hard fork to engender a chain split.[221] With a soft fork, only one blockchain remains valid as users adopt the update. With a hard fork, two concurring blockchains are created, and users are required to upgrade to the latest version of the software. In either of these scenarios, colluders would "erase" the information on the blockchain by adopting the newest version of the blockchain where the information related to the collusion would be altered. Alternatively, colluders could adopt a blockchain with a backdoor allowing them to change a block without changing its hash.[222] Purging the risk of detection could also be done by using technologies such as "zero-knowledge proofs."[223] Indeed, if the blockchain records are encrypted using such technologies, it would then be possible for colluders to leave the blockchain without leaving any readable trace of past conduct.

In short, this tendency to move away from self-reporting[224] and towards self-regulation of collusive agreements operating on blockchain is manifested in two ways: (1) collusive agreements are robust during their existence with very few deviant behaviors, and (2) their disappearance is sudden and can be properly achieved by smart contracts causing, in a sense, their heart attack. The partial disappearance of leniency proceedings should therefore not be a major concern in terms of detecting illegal behaviors.[225] Unlike monopolization and abuses of dominance on blockchain, the cooperative nature of collusion combined with smart contracts will (automatically) cause most of collusion to terminate.

[221] See our previous developments on forks, *supra* Section II.A.3.

[222] *See* Gideon Greenspan, *The Blockchain Immutability Myth*, MULTICHAIN (May 4, 2017), https://www.multichain.com/blog/2017/05/blockchain-immutability-myth [https://perma.cc/AYN2-3FB8].

[223] *See* Ben Garfinkel, Recent Developments in Cryptography and Possible Long-Run Consequences 22–23 (2018) (unpublished manuscript), https://www.fhi.ox.ac.uk/govai/#publications [https://perma.cc/UKV8-B5QY].

[224] And thus bypassing the very disturbing moral and historical aspect of denunciation.

[225] On the contrary, European follow-on enforcement, which necessitates first a decision coming from a public authority to introduce a subsequent trial, will likely disappear in such scenarios without being replaced by any blockchain mechanism.

Perhaps in most cases, blockchain will allow a faster dissolution of collusive agreements using smart contracts. Studies suggest that leniency is helpful in detecting non-profitable and poorly designed collusive agreements — in short, those which are about to collapse anyway.[226] Blockchain will do the same, but potentially more rapidly. As such, blockchain combined with the use of smart contracts could be more effective than the leniency procedure is in detecting illegal practices. In other words, a leniency procedure increases uncertainty and makes it more difficult for colluders to reach an agreement by diminishing trust among them.[227] Smart contracts raise the level of certainty (i.e., trust in the collusive agreement governance) by punishing all deviations from the agreement. The mechanisms are opposite, but the primary end-result is similar.

V. Conclusion

Blockchain is a new and yet little-explored territory. It is, amongst other things, the Amazon[228] of tomorrow's collusive agreements: full of different life forms and new possibilities, the technology will give rise to unidentified creatures and dangerous species that we do not really know how to approach.

I have first shown that blockchain will be used to enhance the functioning of collusive agreements as we know them and that new forms of collusion linked to the technology conditions of access and use will appear as well. Second, blockchain will increase the stability of collusive agreements, providing them with a good life. Depending on whether the blockchain is public or private, a double paradox could emerge. One paradox is related to the visibility of all practices to colluders while ensuring their opacity to non-colluders. The other is associated with the fact that collusive agreements will be more robust during their lifetime by eliminating a large proportion of deviant behaviors, but will die in more brutal ways.

For these reasons, one can expect an increase in the number of collusive agreements along with an increase in their profitability, but not necessarily in their duration. The number of leniency applications may also drop because blockchain will reinforce trust during the lifetime of collusive agreements. This is largely due to the potential use of smart contracts because once again, "[o]ne of the greatest checks on crime is not the cruelty of punishments, but their inevitability,"[229] which is precisely what smart contracts provide by automating punishments.

[226] *See Ex Officio Cartel Investigations*, *supra* note 178, at 5.

[227] *See* Wils, *supra* note 219, at 338.

[228] I am here referring to the forest, just to be clear.

[229] BECCARIA, *supra* note 1, at 46.

The time has now come to detect collusion by blockchain and smart contracts, however difficult that may be. I have shown that some blockchains are more likely to induce collusive agreements than others. Antitrust and competition authorities may start with focusing their efforts on these blockchains and creating safe harbors for the others, for instance, by ensuring that no sanction will be imposed under antitrust and competition law for a specified number of years. Antitrust and competition authorities may also, when sending questionnaires to undertakings, ask whether they use blockchain, and if so, what type of blockchain, using which consensus, and for what purpose.

But perhaps it is even more urgent to adapt existing legal toolboxes before they become entirely ineffective, which implies considering a "law is code" approach and, generally speaking, transforming part of antitrust and competition law to become allies to blockchain core developers rather than mere threats.[230] It is said that "it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail."[231] As true as this statement is, all we have in existing laws is one size of pliers. With the wrong tools, the most sophisticated technology requiring great precision will not be as adjusted as it could be. Antitrust and competition agencies are currently not equipped to fight collusive agreements by blockchain. This may cause a legitimacy crisis for antitrust and competition law that may become ineffective sooner than expected. Indeed, it is more than likely that the use of current regulatory tools will be prevented by the technical characteristics of blockchain. Agencies further need to start analyzing code and software programming. Without doing so, most illegal activities on blockchain will remain safe. The same is true for all practices outside of blockchain which use the Internet. To date, antitrust and competition agencies refuse to analyze the programming of platforms and software. This creates a legal loophole and encourages companies to commit anti-competitive strategies precisely here.[232]

Without fundamental research on this subject, palliatives will continue to be present, risking the survival of blockchain[233] — or antitrust

[230] *See generally* Schrepel, *supra* note 57.

[231] *See* ABRAHAM H. MASLOW, THE PSYCHOLOGY OF SCIENCE 15–16 (1st ed. 1966).

[232] This does not mean that antitrust and competition agencies must convict dozens of companies overnight based on the programming of their software. They must first gain expertise, notably by hiring software developers in their litigation teams. We see no sign that they are seriously considering it.

[233] *See* Timothy C. May, *The Crypto Anarchist Manifesto*, ACTIVISM (Nov. 22, 1992), https://www.activism.net/cypherpunk/crypto-anarchy.html [https://perma.cc/H3V2-NTMF] ("The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid," but in the end *"*Arise, you have nothing to lose but your barbed wire fences!").

and competition law.[234] Some propose the creation of an identity management system so that the real identities of blockchain users can be revealed.[235] Others have suggested "adding a regulatory node in the blockchain" to spy on it[236] or imposing fines to the core developers when blockchain is used for illegal activities.[237] Going even further, it has been said that public blockchains "governed by international institutions from the legal tradition" such as the United Nations should be created.[238] But in fact, these solutions are either ineffective or would jeopardize the utility of the technology as its applications rely on the key characteristics that I have exposed in our introduction and that would be challenged by these various initiatives. Let us recall first and foremost that blockchain is a fundamental technology that may create good for the world.[239] The creation of safe harbors[240] and regulatory sandboxes[241] will enable competition agencies to respond quickly to the challenges posed by blockchain, but in the end, only a re-conceptualization of the law will provide a satisfactory answer.[242] Without it, antitrust and competition law will face a second legitimacy crisis arising from the absence of decentralized regulatory mechanisms. After all, how can decentralized transactions be properly regulated by pyramidal rules and institutions?

[234] *See* Thibault Schrepel, *Feds Like Cryptocurrencies and Blockchain Tech, and So Should Antitrust Agencies*, TECHCRUNCH (Dec. 13, 2018), https://techcrunch.com/2018/12/12/feds-like-cryptocurrencies-and-blockchain-tech-and-so-should-antitrust-agencies [https://perma.cc/W2GQ-JMG5] (stating that to some respect, antitrust and competition law must leave its place to coding when the latter is a superior means of achieving policy goals. But coding won't do it all and legal enforcement will be needed in some situations.).

[235] Finney, *supra* note 18, at 716.

[236] Cong & He, *supra* note 127, at 30; *see also* WERBACH, *supra* note 5, at 107.

[237] *See* Aaron van Wirdum, *A Primer on Bitcoin Governance, or Why Developers Aren't in Charge of the Protocol*, BITCOIN MAG. (Sept. 7, 2016), https://bitcoinmagazine.com/articles/a-primer-on-bitcoin-governance-or-why-developers-aren-t-in-charge-of-the-protocol-1473270427 [https://perma.cc/CAG2-K9WD] (stating that this is based on the idea that the developers control the blockchain, which is misguided).

[238] Vlad Zamfir, *Blockchain Governance 101* (Sept. 29, 2018), https://blog.goodaudience.com/blockchain-governance-101-eea5201d7992 [https://perma.cc/N49D-EVMJ].

[239] *See* Matt Ridley, *Amara's Law*, RATIONAL OPTIMIST (Nov. 12, 2017), http://www.rationaloptimist.com/blog/amaras-law [https://perma.cc/5FJ7-Q3GR] ("[W]e tend to overestimate the impact of technologies in the short run, but underestimate them over the long term."); *see also* CHELSEA BARABAS ET AL., DEFENDING INTERNET FREEDOM THROUGH DECENTRALIZATION: BACK TO THE FUTURE? 10–11 (2017), https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/59ae908a46c3c480db42326f/1504612494894/decentralized_web.pdf [https://perma.cc/2F4M-A5QT] (arguing that blockchain is moving the world toward decentralization).

[240] Schrepel, *supra* note 57, at 332–33 (stating that safe harbors could make it harder to use blockchain for illegal purposes).

[241] *See* Lianos, *supra* note 95, at 373–74; Yeung, *supra* note 84, at 232.

[242] *See generally* TOM R. TYLER, WHY PEOPLE OBEY THE LAW (Yale University Press 1990) (stating that people tend to obey the laws that they perceive as fair). Similarly, blockchain results from a will of decentralization, and in this regard, it would only be fair for antitrust and competition agencies to use decentralized mechanisms.

APPENDIX 1. TRUST BY SMART CONTRACTS THROUGH THE EXISTENCE OF COLLUSION

Trust by smart contracts	**At the creation of collusive agreements**	**During the life of collusive agreements**	**Causing the death of collusive agreements**
Type of smart contracts	**What:** smart contracts creating collusion *related to* the conditions of entry and/or the functioning of *the blockchain* **Objective**: collusion about the blockchain itself so to create the most trust between colluders	**What:** smart contracts *preventing* deviant behaviors **Objective:** to ensure trust between colluders by automating transactions and/or the publishing of trustful information	**What:** smart contracts to *force* one deviant colluder *to exit* the blockchain **Objective:** to eject a deviant colluder when the deviation can't be forgiven to recreate a trustful environment
	What: smart contracts ensuring the efficiency of a *traditional collusion* (i.e. whose effects are manifested *outside* of *the blockchain*) **Objective**: collusion using the blockchain as a trustful medium	**What:** smart contracts *correcting* deviant behaviors **Objective**: to impose targeted punishments so to compensate for the deviation and to recreate trust between colluders	**What:** smart contracts allowing one colluder to *exit* the blockchain *at will* **Objective:** to create trust between colluders by providing them an exit door (prevent entrapment)