Artificial intelligence and blockchain: an introduction to competition issues

Gianluca Faella and Valerio Cosimo Romano
Cleary Gottlieb*

1. Introduction

Artificial intelligence (AI) and blockchain are disruptive technologies, which are taking the lead in economic discourse at the international level and promise to reshape entire industries. These technologies offer an unrivalled potential to improve efficiency levels and benefit consumers, also through lower production and transaction costs, more innovation, and the introduction of new and better products and services.

At the same time, commentators and agencies agree that AI and blockchain present theoretical and practical challenges for policy-makers and enforcers. They may facilitate certain anticompetitive practices, raise novel issues and challenge some of the traditional competition analysis tools and concepts. In some cases, the combined use of AI and blockchain may even increase the antitrust concerns raised by these new technologies.

With the contribution of enforcers, lawyers and in-house counsels, with both economic and legal backgrounds, this symposium discusses the competition and regulatory issues arising from the above-mentioned technologies and looks ahead to possible future developments.

2. Artificial intelligence

There is no single definition of AI. In this introduction, we refer to AI as the process of replicating cognitive human functions, such as learning and problem solving, through dedicated hardware. AI is based on algorithms (sets of unambiguous instructions to be executed by hardware) and frequently relies on the use of big data (large and complex information datasets). When appropriately fed by data, the algorithms at the basis of AI can autonomously learn and iteratively improve their performance by learning new heuristics, or can themselves write other algorithms.

AI may work at a speed and accuracy impossible to achieve for humans. However, unlike the human brain, AI lacks commonsense reasoning and, in itself, is indifferent towards ethics and legal compliance. Accordingly, it is no surprise that the use of AI has been questioned from many legal standpoints.

One of these is antitrust. Scholars and commentators are increasingly focusing on the possible antitrust implications of the use of AI technologies. Competition authorities and courts

---

* Gianluca Faella is also associate professor of competition, intellectual property and comparative law at Link Campus University, and adjunct professor of law and economics at LUISS Guido Carli, and Valerio Cosimo Romano is also adjunct professor of principles of civil law at LUISS Guido Carli and of competition law at LUMSA.


have dealt with algorithms in different cases, such as Online sales of posters and frames in the UK, and Topkins in the United States. AI promises to be even more problematic than traditional algorithms: despite the substantial benefits that these technologies may bring to consumers (in terms, for instance, of new products and services, better tailoring to consumers’ preferences, productive efficiencies, and lower transaction costs, due to their data collection and processing abilities), AI may hide different antitrust perils.

The main area of antitrust concern is the use of AI to facilitate or implement forms of coordination. In this respect, different scenarios can be envisaged. First, AI technologies may be used to facilitate and, possibly, implement collusive schemes established via human interaction. In particular, AI can be used to achieve, coordinate and monitor a collusive scheme by signaling firms’ willingness to enter into a collusive agreement, coordinating its implementation, and monitoring compliance. The immedateness and cheapness of processes managed by AI tools, as well as the accuracy and granularity of the information generated by them, may significantly improve the performance of cartels.

More sophisticatedly, willing or inadvertent collusion may be directly reached by software. If different firms elaborate and use algorithms specifically aimed at achieving collusion, their liability under competition rules should be reasonably clear. The assessment may be more problematic when humans set different and as such legitimate goals (e.g., profit maximization), but self-learning algorithms come to the conclusion that coordination is the best option in the firm’s interest.

The self-learning and predictive capacities of sophisticated algorithms may enable firms to immediately adapt their pricing policies to changes in market conditions, thus making tacit collusion much easier to achieve, more stable and, ultimately, more frequent, even among large groups of competitors.

In the realm of unilateral practices, AI could be employed to implement or facilitate both exploitative or exclusionary conduct. In particular, it is commonly held that intelligent pricing algorithms provide huge potential for engaging in discriminatory practices, as they may enable undertakings to collect and elaborate precise information on consumers’ preferences and willingness to pay, in order to implement extremely sophisticated forms of (real time) price discrimination. AI-based discriminatory pricing might even come close to perfect discrimination, through the offer of (almost) personalized prices.

Moreover, AI might facilitate exclusionary practices such as margin squeeze or predatory pricing, by helping firms to estimate competitors’ costs structure and to assess the probability that the practice will be successful and profitable.

Even in the context of mergers, the possible strategic use of AI technologies for anticompetitive purposes should be taken into account. Extremely effective and rapid intelligent adjustment by AI agents may increase the risk that concentrations lead to coordinated effects, even in less concentrated markets.

Some features of AI also raise the question whether it is necessary to adapt traditional legal concepts and competition analysis tools. As noted above, AI technologies may exponentially increase the potential for autonomous intelligent adjustment, which may lead to coordinated outcome in the absence of any meeting of minds in the traditional sense.

Moreover, the allocation of antitrust liability for AI-based anticompetitive practices may be uncertain. See, e.g., M. Dolmans, supra note 1.

6  See, e.g., M. Dolmans, supra note 1.
7  See M. Dolmans, supra note 1.
AI agents cannot be punished in themselves and normally act on behalf and in the interest of firms. In the case of anticompetitive practices implemented by AI agents, the chain of liability may well extend from software or hardware developers to resellers and end users. Answering the question of who must be held liable for anticompetitive decisions and actions of AI agents may be far from straightforward. The solution may depend on the factual and legal context of each case.

The above issues raise the question of whether it may be appropriate for policy-makers and courts to update traditional notions, such as those of “undertaking” or “agreement”, to ensure that anticompetitive practices carried out with the help of, or directly by, AI are actually captured.

Another challenge for enforcers is how to detect and prevent possible anticompetitive uses of AI. In principle, competition authorities can adopt different approaches. A solution might be the use of investigation powers to carry out, also with the help of external experts, a detailed review and assessment of self-learning algorithms’ features and functionalities, taking into account the data being processed and the instructions coded in the algorithms. However, in some cases, interpreting algorithms’ features and functionalities might be extremely complex, and antitrust authorities might have to assess them indirectly, on the basis of the results achieved and their impact on the market. Another possible approach is to ensure antitrust compliance by requiring that AI is designed so as to comply with competition rules.

The question arises whether the need to review and interpret complex and sophisticated IT tools makes it necessary to provide antitrust authorities with additional resources and adjust their recruitment policies.

On the other hand, AI may create new opportunities for antitrust authorities. The latter could use AI technologies as sophisticated tools to detect wrongdoings and monitor compliance with antitrust rules and decisions. For instance, AI tools could be used to monitor and assess market trends and developments, with a view to identifying possible anomalies, which might be linked to collusive conduct or unilateral anticompetitive practices. The use of AI could also simplify and speed up the review process in merger cases or the conduct of antitrust proceedings, and could enable enforcers to monitor more effectively and at lower costs the correct implementation of remedies and commitments by firms.

AI could also be employed in private damages actions, especially to collect and assess evidence. For example, the use of AI tools might facilitate the finding of a causal nexus between the conduct and the damage allegedly suffered, and could help to quantify damages more precisely.

Needless to say, the increasing use of, and antitrust focus on, AI technologies bring important challenges also for in-house counsels, external lawyers and economic consultants, who have to be ready to navigate the evolving regulatory environment, as well as to fully exploit the potential of AI tools in carrying out their activities.

3. Blockchain

Blockchains are digital ledgers used to record transactions across many users (or nodes). A blockchain is formed by a chain of records (or blocks) linked to each other through cryptography. These blocks are authenticated by a mass-collaboration process (mining) and cannot be altered retroactively without altering all subsequent blocks, which would require an agreement by the majority of the network’s users. Thus, they allow peer to peer transactions without having to involve any third-party intermediary. The key feature of blockchain lies in its decentralized nature: all the data are stored ubiquitously across
the network and every user has a copy of the blockchain.

Blockchains are usually classified as public, private or hybrid. Public (or permissionless) blockchains have no access restrictions and the information on transactions can be viewed by all users in the system. The most relevant example of public blockchains are cryptocurrencies, such as Bitcoin and Ethereum. By contrast, private (or permissioned) blockchains can only be joined upon co-optation by their administrators, and the information stored is only accessible to those who have been given permission to participate in the network. Permissioned blockchains are frequently used for business purposes, due to their advantages in terms of governance, privacy and level of security. Lastly, hybrid blockchains combine the design of public and private blockchains, allowing for specific information to remain private.

Blockchains can also be used as virtual machines to execute smart contracts. Smart contracts are self-executing computer scripts that do not require any human input, except for the initial coding and the decision to enter the smart contract on the ledger. Smart contracts can automatically receive the information needed (e.g., register the availability of a given product), perform the preset tasks (e.g., launch a buying order), and implement the subsequent steps (e.g., pay the amount due upon acceptance of the offer).12

In the realm of blockchain, competition may arise at different levels: among different blockchains, among blockchains and non-blockchain substitutable technologies, as well as at different levels of the supply chain, in relation to the input or output related to the blockchain.

Blockchains is a relatively new digital territory and its antitrust implications are still largely unchartered.13 Some possible implications are currently being tested in an antitrust case pending in the US,14 which relates to an alleged agreement between a number of investors, miners and protocol developers to support the enactment of certain rules for a cryptocurrency (Bitcoin Cash). However, this case is still at an initial stage and the publicly available information does not shed much light over the underlying theory of harm.

At a cursory glance, the use of blockchain technologies may have significant beneficial effects. Blockchains are efficient (because they by-pass the need for intermediaries), transparent (because they are often based on open-source code), and reliable (as all the information is checked, approved and registered). In addition, compared to other digital platforms, in principle they are less favorable to the occurrence of market power, as no single firm normally controls the network.16 Nonetheless, the use of blockchain technologies has raised several issues.

Blockchains are not immune from the risks of market power. The oligopolistic structure of mining has already attracted the attention of antitrust scholars.17 The distributed structure of the platform

---

11 See, inter alia, T. Schepel, supra note 2, para. 5.
15 See, e.g., R. Nazzini, supra note 2, para. 5.
16 On the efficiencies created by blockchain technology, see OECD, supra note 2, para. 5.
17 It is estimated that three mining pool operators (group of entities or persons sharing their processing power over a network) currently control 52.5% of hashing power and the six largest operators...
and the links between its members might lead to situations of collective dominance, especially in permissioned blockchains.18 Moreover, firms holding a dominant position in complementary or ancillary markets (mining hardware, digital wallets, off-blockchain services, etc.) could leverage their position to blockchain markets, however defined.19

Many commentators have warned against certain uses of the new technology that may lead to horizontal restrictions of competition.20 In particular, it has been noted that the blockchain technology has the potential to increase colluders’ ability to agree upon, monitor and sanction their respective market behavior,21 in real time and at near-to-zero cost. For instance, cartelists might codify anti-competitive terms and conditions in a smart contract, with a view to raising prices, cutting output, or allocating markets. Smart contracts may also automatically detect and punish deviations from the collusive scheme. Moreover, in private blockchains, smart contracts could ensure the deletion of incriminating data, as the owner of a private blockchain retains the right to override, edit, and delete the entries on the blockchain.22

Blockchains could also be used by competitors to retrieve or exchange competitively relevant information, thus fostering collusive equilibria.23 Trusted price information available on blockchains could be used by self-learning algorithms to set and continuously adjust prices in a (tacitly) coordinated market environment. The interaction of AI and blockchains may thus further increase the risk of coordinated behavior.

Blockchain technologies will also be relevant in the assessment of other practices, such as exclusionary and exploitative abuses. When the new technology becomes a commonly used tool in commercial transactions, competition authorities and courts may have to deal with different practices capable of having anticompetitive effects, such as the exploitation of market power through excessive transaction fees, the refusal to grant access to private blockchains that have become an industry standard, and the offer of very low transaction fees to exclude platforms based on rival blockchains or alternative technologies.

Antitrust authorities will also have to deal with blockchain technology in the assessment of concentrations. The setting up of blockchains, especially private ones (involving the creation of a “consortium”), may amount in themselves to notifiable transactions. Concentrations between firms participating in the blockchain eco-system, active at the same or different levels of the value chain, may raise both horizontal and vertical issues. Furthermore, blockchain’s potential to facilitate tacit collusion may have to be taken into account in the assessment of coordinated effects.

At the same time, blockchain may provide new opportunities for antitrust authorities, such as the possibility to use the new technology to increase the availability and reliability of the evidence to be audited and evaluated during antitrust and merger proceedings and in possible subsequent monitoring phases.24

4. What’s inside

The articles included in this symposium address many of the above mentioned issues.

---

18 See T. Schrepel, Collusion by Blockchain and Smart Contracts, supra note 13; I. Lianos, supra note 10.
19 See OECD, supra note 2, para. 19.
20 See, e.g., T. Schrepel, Collusion by Blockchain and Smart Contracts, supra note 13, and A. Deng, supra note 13. The risk of collusion may depend on the features of the technology concerned. Public blockchains seem to be less conducive to collusion. Higher risks can instead be identified in private blockchains, in particular those formed by consortia including actual or potential competitors.
21 See, e.g., M. Nissen-M. von Haller Granbaek, supra note 12; OECD, supra note 2, para. 17 and R. Nazzini, supra note 15.
22 See, e.g., T. Schrepel, Collusion by Blockchain and Smart Contracts, supra note 13, A. Deng, supra note 13, and M. Ristaniemi - K. Majcher, supra note 13.
23 See, e.g., OECD, supra note 2.
24 See OECD, supra note 2, para. 24.
The papers on AI provide the views of representatives from the Italian Competition Authority (Andrea Pezzoli and Alessandra Tonazzi) and the European Commission (Álvaro García-Delgado), as well as antitrust lawyers (Gönenç Gürkaynak, Timothy Snyder, Kelly Fayne, and Karen Silverman).

Andrea Pezzoli and Alessandra Tonazzi focus on pricing algorithms, discrimination and collusion. They investigate the issues raised by personalized prices and the delicate interaction between privacy, consumer protection and antitrust rules. They also focus on the grey zone between explicit and tacit collusion created by intelligent algorithms, where there seems to be no meeting of minds in the traditional sense, but super-fast and super-rational autonomous adjustment. According to them, in order to find an appropriate balance between ex-post and ex-ante intervention, a more rigorous assessment of coordinated effects in merger cases and regulatory intervention against algorithms designed with a mere anticompetitive objective may be advisable.

Gönenç Gürkaynak provides an optimist view, focusing on the efficiencies created by algorithms and AI. First, he discusses the efficiencies generated by more traditional algorithms, such as lower costs for both consumers and suppliers, more effective pricing strategies, and better and customized products and services. Then, he turns to the substantial efficiencies that may be generated by AI, including a more effective allocation of work, cost savings, more innovation and new products and services. In the author’s view, while algorithms and AI may be detrimental to competition in certain cases, they can also lead to substantial efficiencies and benefit consumers.

Timothy Snyder, Kelly Fayne and Karen Silverman focus on the issues raised by antitrust risk management and compliance in the AI era. In the new scenario, the task for antitrust advisors is to prepare their clients and companies to navigate evolving regulatory environments. To this end, the authors provide some useful recommendations and suggestions on how to interact with AI developers, implementers and users to identify and avoid antitrust pitfalls. According to them, effective dialogue and cooperation with developers, implementers and users on the front lines of AI are essential to deal with a new wave of antitrust challenges.

Álvaro García-Delgado García discusses the EU regulatory strategy on AI and its relationship with competition policy. He focuses on the main features of the European AI strategy, namely (i) the need to ensure ethical and trustworthy AI, and (ii) the urge to unlock data to make the most of it. In his view, the EU strategy clearly differs from those of other countries and geopolitical blocks, in that it is anchored in the need for “ethical by design” technology. Ethical principles and fundamental rights represent focal points of the EU strategy. While many issues arising from the proliferation of AI are mainly of a regulatory nature, competition policy will continue to play an important role, in particular in ensuring data access and interoperability.

The papers focusing on blockchain provide the views of two members of the OECD Competition Division (Antonio Capobianco and Chris Pike), two antitrust lawyers (Falk Schöning and Myrto Tagara) and a senior in-house counsel of a leading IT company (Pietro Acerbi).

Antonio Capobianco and Chris Pike provide a comprehensive and detailed assessment of the possible antitrust issues raised by blockchain technology. They discuss, inter alia, the two-sided nature of these platforms, pricing issues, the exercise of market power by permissionless and permissioned blockchains and related enforcement challenges, possible exclusionary and exploitative practices, and opportunities created by the new technology. They argue that many possible problems behind blockchain are standard concerns already investigated by competition authorities in market settings involving other technologies. In their view, agencies should focus on (i) permissioned blockchains, also by exploring their design protocols, and (ii) the risk that blockchains are excluded, as a result of foreclosure by dominant incumbents or lobbying for disproportionate anti-competitive regulation.

Falk Schöning and Myrto Tagara reflect on the increasing focus of competition authorities on the antitrust issues raised by blockchain technology. They argue that, even though, in principle, existing competition law tools and concepts are
sufficiently flexible and fit for the purpose of analyzing blockchain cases, antitrust authorities may face some challenges in their enforcement. In particular, they discuss some problems that may arise in identifying the liable entity, defining the relevant market, assessing dominance and possible anticompetitive practices, and determining to which entity a decision should be addressed.

Lastly, Pietro Acerbi provides an interesting view from the business’ perspective. He considers that blockchain is a disruptive technology, which may revolutionize traditional transaction models. After discussing some potential applications of blockchain technology in cryptocurrencies, supply chains, and finance, the author turns to the legal issues, namely those related to competition law. In his view, the new technology as such does not truly raise prohibitive antitrust law challenges. Technical measures can be implemented at the design stage to address and prevent possible risks. In addition, it is important to ensure that blockchain mechanisms and data management mechanisms are explainable and transparent to authorities, if needed. From this point of view, corporate responsibility and transparency are key.

Ultimately, AI and blockchain are sophisticated, powerful and disruptive tools, but still tools in the hands of firms. What really matters is how they are employed by firms and for what purposes.