The Challenges of Blockchain Technology to Competition Law

Christophe S. Hutchinson

Senior lecturer, Department of Legal Regulation of Economic Activities, Financial University under the Government of the Russian Federation. Address: 49 Leningradsky Prospekt, Moscow 125993, Russia. E-mail: sam_hutch2004@yahoo.fr; KSYUchinson@fa.ru

Abstract

Blockchain is a catch-all term for a combination of three technologies: distributed ledger, cryptology and network protocols. The first enables storing the same info in different places, the second allows secure transactions to be recorded and then encrypted on the distributed ledger. The third element governs the network and verifies transactions across the network automatically and independently. Considered by many as "the biggest technological innovation since the Internet"[1], blockchain is a decentralized, more secure and transparent model for transactions that operates on an encrypted peer-to-peer basis. This model makes trust between parties superfluous by instead placing trust in the underlying technological platform. This would effectively remove the need for intermediaries whose business has been to make up for the lack of trust; these include banks, brokers, governments, internet platforms, law firms etc.[2] While reducing the costs of contract enforcement and thus facilitating trade, blockchain technology may have significant implications for antitrust law. As decentralized organizations such as blockchain are not recognized as legal persons, this raises questions about whether anticompetitive practices and their perpetrators can be identified. For example, can a non-entity hold a dominant position? Can blockchain create a "monopoly without a monopolist"? Finally, if a blockchain is dominant, which users and/or entities hold that dominant position? This article intends to highlight the challenges that blockchain presents to the analyses of unilateral anticompetitive practices[3].

Keywords

distributed ledger, cryptology, network protocol, immutability, antitrust, public and private blockchain, dominant position on the relevant market, abuse of dominance, exclusionary abuse, exploitative abuse, discriminatory abuse.

[1] *Medcraft G.* Blockchain or distributed ledger technology: The biggest technological revolution since the Internet. 2018. Available at: https://podtail.com/en/podcast/oecd-on-the-level-podcast/the-blockchain-revolution-the-power-of-positive-di/ (accessed: 26.05.2020)

[2] *Penz-Sharp A.* Blockchain for Business: Ready or Not, Here it Comes, *CMS Wire*, 4 December 2017. Available at: https://www.cmswire.com/information-management/blockchain-for-business-ready-or-not-here-it-comes (accessed: 01.07.2019)

[3] Cartels are excluded from this study in order to keep this article to a reasonable length. Many of the points made in this article can nonetheless be applied to cartels.

For citation: Hutchinson C.S. (2020) The Challenges of Blockchain Technology to Competition Law. *Legal Issues in the Digital Age,* no 1, pp. 32–53.

Introduction

Blockchain is a general-purpose technology that threatens to disrupt markets and institutions across the world. While Internet enabled the publishing and digital transfer of information, blockchain by ensuring the trust necessary to undertake transactions and reducing uncertainties (through its use of dependable self-executing code) makes it possible to identify the ownership of assets, make them unique and traceable, and facilitate digital transfers that then enable exchanges of assets.

The World Economic Forum predicts that 10% of global gross domestic product will be stored on blockchain by 2027[4]. Blockchain's attractiveness lies in its ability to drastically reduce the transactional costs[5] required to create trust between parties through recourse to intermediaries such as banks, brokers, governments, internet platforms, law firms, legal procedures, etc.[6] It can indeed facilitate making contracts and mitigate widespread contractual inadequacies[7] by creating a world in which "computers... fill the gaps of contracts" [Schrepel T., 2018: 15].

Although it facilitates trade, blockchain also presents numerous legal challenges with substantial implications for antitrust law. One of these challenges is suggested by the word "antitrust" itself. On the one hand, a large part of competition law is referred to as *anti*-trust, using the American terminology that emerged as a reaction to the misuse of the trust instrument [Ernst D., 1990: 879]. On the other hand, blockchain technology eliminates

[4] World Economic Forum. Technology tipping points and societal impact, survey report 24. 2015. Available at: https://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf (accessed: 23.03.2019)

[5] *Roberts R., Epstein J.* On bitcoin, the blockchain, and freedom in Latin America. *ECON TALK*.13 February 2017. Available at: http://www.econtalk.org/jim-epstein-on-bitcoin-the-blockchain-and-freedom-in-latin-america/ (accessed: 13.05.2019)

[6] *Penz-Sharp* A. Blockchain for business…

[7] *Cong L., He Z.* Blockchain disruption and smart contracts. 27 December 2018, p. 4. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764 (accessed: 26.05.2019). "[B]lockchains, via decentralized consensus, enable agents to contract on delivery outcomes and automate contingent transfers. Hence, the authentic entrant is now able to signal her authenticity fully. This eliminates information asymmetry as a barrier for entry and greater competition, enhancing welfare and consumer surplus in this blockchain world."

the need for a fiduciary, that is, a person who creates trust, because it works automatically without any physical or artificial person[8]. What happens when antitrust law confronts a technology that works without a trusted counterparty? Is it time to leave behind both the regulatory apparatus of antitrust? From a legal point of view, are the current rules well suited to analyzing blockchain and its processes?

This article intends to highlight the challenges that blockchain presents for analyzing unilateral anticompetitive practices. It is divided into two parts, the first of which describes how blockchain functions. The paper then argues that, because blockchains are anonymous, immutable and decentralized, questions arise about whether anticompetitive practices and their perpetrators can be detected.

1. How Blockchain Functions

This section focuses only on the fundamentals of blockchain's operations, highlighting those that are particularly relevant for antitrust analysis. In addition, this part deals with the distinction between public and private blockchains, which is important because of the implications of this distinction with respect to competition law. Finally, it explores the differences between Blockchain 1.0, 2.0, and 3.0 to show how blockchain is used today and what direction it may take in future.

1.1. General Aspects

Blockchain is a catch-all term for a combination of technologies which have come together to create networks that are capable of securing trust[9] between people that have no antecedent reason to trust one another. Blockchain combines the following three technologies: distributed ledger [Raval S., 2016: 21] cryptology and network protocol. Distributed ledger allows the storing of the same information in different places [Posner E., Weyl G., 2018: 368]. Although the cryptology that was created during World War II is

[8] *Murck P*. Who Controls the Blockchain? *Harvard Business Review*.19 April 2017. Available at: https://hbr.org/2017/04/who-controls-the-blockchain (accessed: 13.05. 2019)

[9] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system.2008. Available at: https://bitcoin.org/bitcoin.pdf (accessed: 12.05.2019). In the words of Nakamoto, blockchain is based on "cryptographic proof instead of trust."

nothing new[10], it enables encryption of transactions or data on a distributed ledger. By combining distributed ledgers and encryption, parties can trust one another. The third element, which is a new one, is network protocol [Dannen C., 2017: 3]. It governs the network and verifies transactions or data transfers across a network independently and automatically. By loading a protocol onto a computer, a person becomes a node in the network. The network protocol thus allows verification of what is in the network. A transaction or a transfer over the network is carried out when one party sends data, such as a digital coin or a piece of data, to another party over the network. Every time there is a change in the ownership of an asset due to this transaction a new block is added to the already existing blocks. All these blocks are linked cryptographically forming a chain through which it is possible to trace an entire transaction of any particular asset.

Blockchain has several advantages: first, it is *decentralized*. The network exists across a series of nodes formed by the computers that store the blockchain information and also contribute to verifying the transactions. When a transaction takes place, parties on both sides of the transaction interact with each other through peer-to-peer transmission, with communication being done directly between them and not through a central point. The nodes are like a "bunch of people sitting around saying: yes, yes, thumbs up, we all agree"[11] to the transaction being carried out on the network. The decentralization means that *no single participant controls the information* on the blockchain.

A second advantage of blockchain is that it is in principle *visible to all,* which means that all users on a blockchain can see all the transactions regarding an asset being traded on the blockchain and who holds an asset at any particular time[12.]

Third, it is *anonymous* [Champagne P., 2014: 136] as no user has to provide a name, an e-mail address, or any other personal data in order to download and use the network software [Tapscott D., Tapscott A., 2016: 282].

Lastly, blockchain data is also *immutable* [Walch A., 2017: 713]. Once information is stored on a block, it cannot be tampered with by individual participants unless the whole network agrees to such a change.

[10] Medcraft G. Op. cit.

[11] Ibid.

[12] Most of the data put on the blockchain is encrypted so that only people with the right keys can decrypt it. However, the "visible effect" remains the rule and the protocol design is visible by all.

1.2. Public vs. Private Blockchain

There are different types of blockchains. The difference comes down to whether the information stored on the blockchain is public or private and whether potential nodes and users on the network need permission to join or not. There is a taxonomy on public/private and permissioned/non-permissioned blockchain.

Public blockchains[13] such as Bitcoin and Ethereum are open to all. To become a node on those networks, each participant needs to set up their computer by implementing the governing protocol. They can remain pseudonymous behind a unique user identifier within the network. The ledger tracks each participant by their identifier. The ledger is transaction-based, and it notes the prior transaction history. This information can be used to assess whether the participant has sufficient funds, capacity, inventory, etc. to complete the requested transaction based on the prior transactions that either have credited or debited the account.

Anyone can propose blocks of transactions to be added to public blockchains. There is no central validation system that oversees the blockchain to determine which blocks of transactions get added or to determine which are valid when discrepancies occur. Instead, blockchains use present rules, a "consensus mechanism", to decide which record should prevail.

For example, the party on the Bitcoin blockchain that is the first to correctly solve a computational puzzle gets to propose the next block to the network. This is called "mining". The nodes on the network signal their acceptance of the proposed block by adding it to their copies of the blockchain after validating that the computational puzzle was solved directly, that the transactions in the block are valid, and that the bitcoin in each transaction was not previously spent. If there is a conflict between different versions of the blockchain, the chain that has the largest amount of computational work is considered to have the accurate record under a "proof of work" protocol. Under this system, there is no practical likelihood that one participant can be strategically prioritized or given an unfair advantage over another. To the extent disputes arise between participants, there are no default rules to resolve them[14].

[13] Public blockchains are also called "permission-less" or "open" blockchains.

[14] Thomas R. Blockchains and antitrust: New technology, same old risks . Available at: https://www.jonesday.com/blockchains-and-antitrust-new-technology-same-old-risks-08-02-2018/ (accessed: 16.05.2019)

A public permissioned blockchain is a system in which the information is public but entering new information or verifying a new transaction requires permission from a central authority. Such is the case, for instance, with a blockchain used for land registry. Any potential buyer can consult it and check the identity of the owner of a particular piece of land, but in order to make an entry in the registry the buyer must have the right permission. This type of blockchain is public because everyone can see who owns the land and it is permissioned to the extent that changes of property require permission from the state. The practical implications of this type of blockchain are huge. The Swedish government, for instance, is currently looking at a public permission blockchain as a way to collect land tax more efficiently because it is up-dated all the time and it permits linking the land registry blockchain to GPS coordinates[15].

A private blockchain, also called a permissioned blockchain, is a blockchain that restricts reading permissions to certain participants. In such a system, nodes are authorized by a central authority and the information can be used only by the members of the network because it is private. The central authority need not be a single entity. A group of entities is often a feature of a private blockchain. For example, this kind of permissioned blockchain has been used by the banking system for interbank transactions, clearing or settlement, or transferring accounts between insurance providers. In this type of blockchain, there are "full" nodes that actually own an entire copy of the ledgers and "light" nodes that have elements of the ledger, as is often the case in a private blockchain. For instance, a stock exchange owns all the ledgers that are in that system and an operator, in its capacity as owner of an equity or security, will have access only to their particular part of the chain, which is their account in it.

Private blockchains are subdivided into two different categories. The first is called a single entity blockchain. As its name suggests, a single entity will set up the protocol and run the blockchain, while reading permission may be public or restricted to certain participants. The second category is called a consortium blockchain. The consensus process in these is controlled by a pre-selected set of nodes. For example, the consensus mechanism could be made up of five companies, each of which operates a node, with three of them required to sign in order to validate a block. Regardless of the techni-

[15] Medcraft G. Op. cit.

cal particulars, all consortium blockchains operate under the leadership of a group instead of a single entity. In addition to private and public blockchains, there are also semiprivate blockchains. Those blockchains are run by a single company that grants access to any qualified user.

1.3. Consensus and Governance

Blockchains can be classified by the way they achieve consensus. The consensus mechanism is the general agreement, unanimous by nature, under which the blockchain works. The integrity of the blockchain relies on the chosen consensus to clear transactions.

Several major public blockchains (e.g., Bitcoin and Ethereum) currently use a form of consensus based on proof of work, in which certain users who are referred to as miners in these systems compete in solving a cryptographic puzzle in order to be chosen to verify the integrity of transactions [Vigna P., Casey J., 2018: 39]. The first to solve the puzzle is rewarded with a transaction fee. Many public blockchains are currently working on developing a "proof of stake"[16] consensus derived from cryptoeconomics and game theory [Kreps D., Wilson R., 1982: 253].

With private blockchains, however, there is generally no mining, no proof of work, and no remuneration. The benefits of a private blockchain come from its applicability to value. Uses of private blockchains include: (1) serving as a way to transfer value (currency, securities, votes, industrial patents, the Internet of Things (IoT), stocks, and bonds)[17]; (2) serving as a register to verify the exchange of products and assets[18]; and (3) serving as a smart contract by enabling an automatic program to insert terms and conditions [Cuccuru P., 2017 :179].

[16] *Zamfir V.* Introducing Casper "the Friendly Ghost", *Ethereum Blog*. 1 August 2015. Available at: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost (accessed: 10.05.2019). "In it, the algorithm attempts to solve these problems by removing the mining concept entirely and replacing it with another mechanism. With the proof of stake, the same participant invests $1,000 by directly purchasing the cryptocurrency of the blockchain then deposits these cryptocurrencies using the proof of stake mechanism, which will then (pseudo-) randomly assign that participant the right to produce blocks and receive a reward." In short, the so-called "Casper Protocol" is set to transfer Ethereum from a proof-of-work to proof-of-stake model in the coming months.

[17] *Guegan D*. Public blockchain versus private blockchain. Documents de travail du Centre d'Economie de la Sorbonne.18 March 2017. Available at: https://halshs.archives-ouvertes.fr/halshs-01524440/document (accessed: 09.05.2019)

[18] Ibid.

Whoever controls the consensus — also known as the consensus mechanism — controls the governance of the blockchain [Huberman G., 2017: 3]. The consensus operates and communicates between network nodes. For instance, Dash[19], a crypto-currency, uses a governance system that allows its users to vote if they hold tokens. Decred, also a crypto-currency, has a more centralized governance system according to which some of its users, called the Masternode, have more power within the community. A blockchain's ability to implement anticompetitive strategies will vary depending on its governance system.

1.4. From Blockchain 1.0 to Blockchain 3.0

Antitrust concerns about blockchain platforms and the software operating on them pertain to different types of anticompetitive practices: those that are committed via the blockchain itself as a platform; and those that are committed via the applications running on the blockchain.

Not all blockchains allow software (called "layer 2") to run on top of their root blockchain ("layer 1") but most do. Ethereum, for example, is a root blockchain that allows any type of software layer. In fact, Ethereum was designed specifically to allow users to create "smart contracts" [Dannen C., 2017: 3] or agreements between accounts to automatically transfer tokens when certain conditions are met. Anyone can upload a program onto this platform and leave it to self-execute securely [Tapscott D., Tapscott A., 2016: 221].

These blockchain applications fall into three generations. The first, Blockchain 1.0, is similar to a currency and includes "cash, such as currency transfer, remittance, and digital payment systems" [Swan M., 2015: 23—34]. The second, Blockchain 2.0, is a contract, including "stocks, bonds, futures, loans, mortgages, titles, smart property, and smart contracts". This category includes all blockchains allowing applications that enable these financial activities. Finally, Blockchain 3.0 includes all "applications beyond currency, finance, and markets — particularly in the areas of government, health, science, literacy, culture, and art" [Swan M., 2015: 51].

These three types of applications (Blockchain 1.0, 2.0 and 3.0) can be developed freely on most blockchains.

[19] Available at: https://www.dash.org (accessed: 04.05.2019)

2. Challenges to Competition

Blockchain sets two main types of competition challenges: it complicates both the characterization of dominant market positions and the attribution of liability for anticompetitive practices. This is particularly concerning because anticompetitive practices are expected on blockchain, as demonstrated below by analyzing how and why monopolization practices might be implemented on it.

2.1. Characterization of a Dominant Position on the Relevant Market

The definition of a relevant market is a tool to set the boundaries of competition between firms by taking into account their material and geographical dimensions. Setting the boundaries of the relevant market can be challenging.

Blockchain raises important questions about what exactly a dominant position is. And because decentralized organizations like blockchain are not recognized as legal entities [De Filippi P., Wright A: 2018: 209], many issues arise. Can a non-entity hold a dominant position? Can blockchain create a "monopoly without a monopolist?" [Huberman G., 2017: 2]. Finally, if a blockchain is dominant in a market, which users and/or entities hold that dominant position?

Unless an entity holding a dominant position is deemed fully liable for all the practices implemented within it, liability will be attributed in different ways that depend on how a dominant position is characterized. The same is true for blockchains: the way in which the dominant position is characterized will determine the scope of liability.

A number of characterizations of dominance could be applied to blockchains. As far as the material dimension of relevant markets is concerned, different theories of liability are conceivable.

The first theory of liability would be to consider that each blockchain — as a general ledger on which transactions are registered — would hold a dominant position in and of themselves. If this were the case, all users of the blockchain would be considered co-holders of this dominant position. In practice, however, it would be illogical to consider all blockchain platforms as having a dominant position while attempting to prevent the implementa-

tion of anticompetitive practices by a fraction of their users. Applying this definition of a market would very significantly reduce the incentive to use blockchains because unwitting users could be held liable for practices performed by third parties unknown to them. Therefore, this first way of defining dominant positions should be rejected.

A second theory would assess market power based on the type of applications (products and services) that run on the blockchain as layer 2[20]. The type of blockchain (1.0, 2.0 or 3.0), which are different strata of smart contracts [Raskin M., 2017: 305], would then be at the center of a market definition that takes into account the two—sided nature [Rochet J.-C., Tirole J., 2003: 990] of the market by analyzing the functioning of applications. In particular, a layer 1 blockchain as a platform would be part of a different market because it does not compete with a layer 2 application.According to this approach, a blockchain's market power would be assessed in comparison with other digital products or services and potentially with non-digital alternatives. As a result, blockchain power would be evaluated the same way online sales can be integrated into the general sales market (including physical sales).

Such a characterization of a dominant position would make it possible to impute liability only to users who offer, run, or use a dominant application that has implemented an anticompetitive practice. This would then allow antitrust authorities to make a distinction between three key players on the blockchain: developers, users, and miners, depending on who commits the anticompetitive practice.

However, this fails to answer the question of which elements to take into account in order to evaluate the relative market power of different blockchains running the same type of applications: the number of users, the number of transactions recorded, the number of blocks, or the revenues, etc. In its Google decision, the court noted that the European Commission used market shares by volume as a proxy for several reasons. "First, market shares by value cannot be computed because general search services are provided free of charge to the user. Second, despite its best efforts, the Commission has been unable to obtain precise and verifiable values regarding the Rev-

[20] A further distinction would be made on whether the blockchain allows the realization of a service taking place outside of the technology, or whether it provides a service within the blockchain. In the first case, it will have to be determined whether the blockchain can be integrated into a wider market — as is the case, for example, with online sales that can be integrated into the general sales market (including physical sales). In the second case, only competition between blockchains would have to be evaluated.

enue Per Search ("RPS") of the main general search services. Third, advertisers look at usage shares when deciding where to place their search advertisements" [Schrepel T., 2019: 275].

In assessing the geographical reach of the relevant market, it should be emphasized that, although the language used on a blockchain is universal, some applications may be focused on a local market while others may compete at an international level. Only a case-by-case analysis is possible here.

In short, evaluating the market power of a blockchain network creates new challenges, one of which is the lack of a central power needed to urge the majority of blockchain users to adopt changes, a characteristic which greatly mitigates the idea of "power"[21].

2.2. Abuse of Dominance

This section focuses on the different types of unilateral practices (exploitation, exclusion, and discrimination) which may occur with blockchains. Before analyzing these unilateral practices in greater detail, two common trends are worth highlighting.

All information and transactions recorded on public blockchains are, to some extent, visible by all[22]. With regard to private blockchains, the transactions are visible only to their users if they are designed that way[23]. As a result, the number of anti-competitive practices may be lower on public blockchains than in other tech markets, precisely because public blockchains create greater transparency between users.

[21] This is seen, for instance, with Ethereum, which has to convince its own users to adopt upgrades to the software. See: *Kim C.* Ethereum upgrades as hard forks activate on blockchain, *coindesk*. 28 February 2019. Available at: https://www.coindesk.com/ethereumupgrades-as-hard-forks-constantinople-and-st-petersburg-activate-on-blockchain (accessed: 24.05.2019). Note that when a blockchain is changing its functioning rule, such as the protocol consensus, all blocks validated according to the new rules are seen by the blockchain software as being invalid. For that reason, all nodes need to upgrade their software to the new rules.

[22] Most of the data put in the blockchain is encrypted so that only people with the right keys can decrypt it. However, the "visible effect" remains the rule and the protocol design is visible by all. Therefore, when anticompetitive practices are set up in the blockchain, that information is visible. Only the manifestation of that practice may be encrypted.

[23] Privacy-oriented blockchain-based cryptocurrencies widely use «zero knowledge proof,» which provides trust. Trust in the system is also ensured by the fact that transactions are visible by all users. The more there are, the more trust there is in the blockchain and the higher its utility. It is therefore uncertain whether private blockchains will, in the future, make transactions non-visible.

Accordingly, it is to be expected that, because transactions can be viewed by all users on the blockchain, this inherent transparency tends to prevent anti-competitive practices and reduce their occurrence. But vigilance is required because unilateral practices will not entirely disappear due to a second pattern in blockchain known as the "opacity effect." On a blockchain, all transactions are encrypted [Werbach K., 2018: 45], and the identity of blockchain users is protected by pseudonyms. As a result, a transaction may be visible, but the nature and purpose of the transaction are unknown to outsiders, and this makes the interaction between users more opaque. This "opacity effect" is even stronger on private blockchains where the content of the blockchain is kept hidden from outsiders.

To demonstrate which unilateral practices could be implemented on blockchain, suppose that company Y is operating in a digital market. Y decides to diversify its activities and creates a private blockchain to do so. Y designs the blockchain so that Y can choose which users may access the blockchain, which operations the users can perform on it, and which protocol will govern the blockchain. Y has the power to change these settings at any time. To generate revenue, Y has developed a new professional social network called BlockJobs that operates as a layer 2 on its blockchain. BlockJobs enables users to post job offers and/or to apply for them. At each stage of the recruitment process — from the first interview to the acceptance or refusal of an offer — a smart contract is recorded on the blockchain. Everything is conveniently automated, but the registration of each of these transactions has a cost that its users looking for candidates pay with tokens. After a while, this application attains great success, and Y realizes that some of its competitors are using BlockJobs to recruit candidates that will enable them to better compete with Y. In response, Y implements an anticompetitive strategy and might adopt such practices as refusal to deal, tie-in-sales, predatory pricing, margin squeeze or exclusive dealing and rebates.

2.2.1. Exclusionary Abuse Practices

2.2.1.1 Refusal to Deal

Article 102 of the Treaty on the Functioning of the European Union (TFEU), which prohibits the abuse of dominant position, can be triggered when a monopolist refuses to deal with a competitor. Although a company

generally has no duty to deal with its rivals, the European Court of Justice has found antitrust liability when a monopolist refuses to sell a product to a competitor although it made that product available to others.

Refusal to deal is a common practice outside of blockchains, but it should be rarer in them, at least when it comes to public blockchains. A refusal to grant access to a blockchain would have to be implemented in its governance design, although by definition a public blockchain is coded to allow public access. No deliberate or exclusive selection of users is possible. As a result, the refusal to deal can be made possible only by modifying the access rules themselves. Exclusionary strategies are therefore incompatible with the inherent nature of public blockchains, and the blockchains that implement them would no longer be considered public ones.

In contrast, the refusal to grant general access is an essential characteristic of private blockchains[24]. Within such permissioned blockchains, the gatekeeping mechanism may take various forms (e.g. preventing a competitor from accessing blockchain information, proposing or registering new transactions, validating the blocks, etc.) and can be managed by different types of actors depending on the governance choices. For instance, a "[r] refusal to access the blockchain might be used to exclude maverick firms or new entrants" and, in general, to "exclude or raise the costs of rivals outside of the consortium"[25]. In order to illustrate a situation of refusal to deal (not allowing an entity to join a blockchain community), imagine that a blockchain exists among European banks for interbank payments. There may exist another way — the old way — of clearing interbank payments that is valid but slow and costly in comparison. If a new bank wanted to set up business in Europe, being a member of the blockchain may be necessary if it intends to become a competitive force. If the new bank is refused access or membership without justifiable grounds or on a cost basis that is not objective and reasonable, this might constitute an abuse[26] within the meaning of Article 102 of the TFUE.

[24] See note 5.

[25] OECD. Blockchain technology and competition policy (2018). Paper by the Secretariat. Available at: https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf (accessed: 03.05.2019)

[26] *Desal K*. Blockchain and competition law, Ernest&Young Law Alert, EU competition law April 2018. Available at: https://www.ey.com/Publication/vwLUAssets/ey-blockchain-and-competition-law/$FILE/ey-blockchain-and-competition-law.pdf (accessed: 3.05.2019)

If a permissioned blockchain attains the status of essential infrastructure and if refusal to give access to it is not properly justified, the exclusionary efforts of the gatekeepers also risk violating Art. 102 of the TFEU[27].

2.2.1.2. Tying/Bundling

Tying or bundling is the practice of making the sale of a product (or service) conditional on additional sales or obligations[28]. Tying may also entail subjecting a contract to the acceptance of supplementary obligations that have no connection with the original subject of the contract.

Tying or bundling is unlikely to occur in public blockchains because by definition they can be freely accessed or used. Making conditional its use to the purchase of a product is therefore unlikely.

On the other hand, private blockchains may that are created by for-profit companies have an interest in imposing tying or similar practices. Bundling may occur if an undertaking links the use of a blockchain (specializing, for instance, in mining a particular cryptocurrency's tokens) to ancillary services (e.g. a digital wallet or exchange service) which are offered outside the blockchain and in which the undertaking holds a dominant position. Tied sales are to be expected on private blockchains.

2.2.1.3. Predatory Pricing

Attempting to drive a smaller competitor out of a market by systematically undercutting its prices is another anticompetitive practice[29]. Pricing

[27] *Ristaniemi M.* & *Maicher K.* Blockchains in competition law-friend or fore? Kluwer Competition Law Blog, July 21, 2018. Available at: http://competitionlawblog.kluwercompetitionlaw.com/2018/07/21/blockchains-competition-law-friend-foe/?print=pdf [accessed: 19.04.2019]

[28] For an overview of tying, see Case 3/37.792, *Microsoft Corp*., Comm'n Decision (Apr. 21, 2004). For American cases, see *Jefferson Parish Hosp. District No. 2* v. *Hyde*, 466 U.S. 2, 1 (1984); *United States* v. *Microsoft Corp*., 253 F.3d 34 (D.C. Cir. 2001). Though the U.S. seemed to adopt the rule of reason after Illinois *Tool Works Inc.* v. *Independent Ink*, *Inc.*, 547 U.S. 28 (2006), "the general per se rule for tying arrangements when market power is present very likely still survives," per Hovenkamp H. The Rule of Reason, *Florida Law Review,* vol. 70, pp. 81, 96. For more on bundling, see *Economides N., Lianos I.* Elusive Antitrust Standard on Bundling in Europe and in the United States in the Aftermath of the Microsoft Cases. *Antitrust Law Journal,* vol. 76, p. 483.

[29] In the European Union predatory pricing is considered abusive if the prices charged by the dominant undertaking are below average variable costs or if the prices charged by the dominant undertaking are below average total costs and they are set as part of a plan for eliminating a

for blockchains typically takes the form of costly transaction fees when a user is submitting a transaction to be registered in the chain. Predatory pricing is very unlikely on public blockchains because it would be possible only if enough users could be persuaded to change the governance structure to accommodate such a change.

The situation could be quite different for private blockchains. For example, a large block validator or a mining pool might set transaction fees below cost in order to eliminate a rival cryptocurrency, or it might cross-subsidize certain key merchants and suppliers in order to prevent a competing cryptocurrency from reaching an efficient scale and generating enough profit to enter the market. These practices may be successful as they will not usually require the dominant undertaking to sacrifice profits. The predatory pricing test according to which if the prices charged by the dominant undertaking are below average variable costs and are set as part of a plan for eliminating competitors, would then apply.

2.2.1.4. Margin Squeeze

Another related practice occurs when a vertically integrated dominant company operates on upstream and downstream markets and sets the upstream price high enough so that companies are unable to sustainably compete in the downstream market[30].

In contrast to private blockchains, public blockchains are by definition horizontal. It is therefore very unlikely for a margin squeeze to be imple-

competitor. See Case C-202/07 P, *France Télécom* v. *Comm'n*, 2009 E.C.R. I-2369. In the United States, in order to establish predatory pricing, the plaintiff must show below-cost pricing and a dangerous probability of recoupment by the monopolist once the rival has been driven from the market. See *Brooke Group Ltd. v. Brown & Williamson Tobacco Corp*., 509 U.S. 209, 223—24 (1993).

[30] Commission of the European Communities. Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings. 3 December 2008. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52009XC0224%2801%29 (accessed: 4.05. 2019). This states that margin squeeze occurs when a dominant undertaking may charge a price for the product on the upstream market which, compared to the price it charges on the downstream market, does not allow even an equally efficient competitor to trade profitably in the downstream market on a lasting basis.

See also: Case C-52/09, *Konkurrensverket* v. *TeliaSonera Sverige AB* 2011 E.C.R. I-527; Case C280/08 P, *Deutsche Telekom AG* v. *Comm'n* 2010 E.C.R. I-9555; and Case C-295/12, *Telefónica* and *Telefónica de España* v. Comm'n 2013 E.C.R. 619. In the United States, a margin squeeze does not constitute an independent cause of action under Section 2 of the Sherman Act. See: *Pac. Bell Tel. Co.* v. LinkLine Commc'ns, Inc., 555 U.S. 438 (2009).

mented on public blockchains. The case is different, however, for private blockchains. Because they allow income-generating applications while maintaining a financial interest in the platform layer, one can imagine that a strategy of margin squeezing could be implemented. Doing so would require that the dominant company — here the blockchain gatekeeper — changes the price it charges in the upstream market (i.e. the blockchain platform). In the development phase of a blockchain, such a strategy seems unlikely, but the potential for it means that it will have to be closely monitored in the years to come.

2.2.1.5. Exclusive Dealing

Another practice which falls under the prohibition in Article 102 of the TFEU consists in the requirement that a supplier with monopoly power over its customers not make abandoning a competitor's blockchain a condition for use of its blockchain to complete transactions[31].

Terms to that effect could be included in the user agreement to be signed before using the blockchain[32]. It seems unlikely that such exclusive dealing will be imposed on a public blockchain because it would entail incorporating exclusionary terms from the start. Moreover, once a transaction is registered on a blockchain, users have little interest in registering the transaction on another blockchain because doing so is costly. The technology itself reduces the incentive to use several blockchains for the same transaction.

The situation is quite different for private blockchains. Foreclosing competitors is an efficient way to increase the overall blockchain price to users and developers. Moreover, private blockchains have an interest in increasing their level of attractiveness by obtaining data that they alone can provide. In the BlockJobs illustration, Y may want to be the only company listing a certain type of job offer. BlockJobs therefore might want to impose exclusive

[31] For an overview of exclusive dealing, see: Case T-155/06, *Tomra Sys. ASA & Others* v. *Commission* 2010 E.C.R. II-4361, and Case C-413/14 P, *Intel Corp.* v. Commission, 2017 E.C.R. 632. In the United States, exclusive dealing may constitute a violation of Section 2 of the Sherman Act if it forecloses competitors from accessing the market. The D.C. Circuit held that "a monopolist's use of exclusive contracts, in certain circumstances, may give rise to a § 2 violation even though the contracts foreclose less than the roughly forty percent or fifty percent share usually required in order to establish a § 1 violation." *United States* v. *Microsoft Corp*., 253 F.3d 34, 70 (2001).

[32] For an example, see: Ethereum Foundation. Legal Agreement on the Ethereum.org website. Available at: https://www.ethereum.org/ (accessed: 18.05.2019)

dealing at the entry point of its blockchain. For this reason, it is very likely that exclusive dealing practices will be implemented on private blockchains.

2.2.1.6. Rebates

Yet another related practice is to grant retroactive rebates or rebates that are contingent on a customer obtaining all or most of its goods or services from the dominant actor[33]. Because all practices are recorded and visible on public blockchains, one user's discount will be visible to all and granting loyalty rebates or discounts could lead to pushback from users who do not benefit from such a discount. This is more likely to occur if such benefits are perceived as unjustified by other users. Public blockchains push for equal treatment of all users when there is no reason to differentiate among them.

Private blockchains do not necessarily benefit from this "visibility effect" because they can determine what information is visible to each user. They may also have a greater commercial incentive to attract reputable users by offering discounts. In the BlockJobs example, Y may want to give a discount on transaction registration fees to some big users. Rebates are, therefore, expected to be employed on private blockchains.

2.3. Exploitative Abuses

Exploitative abuses could be implemented on a blockchain by directly or indirectly imposing unfair conditions on existing customers or suppliers[34]. An exploitative abuse could occur when blockchain creators provide

[33] For an overview of loyalty rebates, see: Case C-413/14 P, *Intel Corp.* v. *Comm'n*, 2017 E.C.R. 632; Case 85/76, *Hoffmann-La Roche and Co. AG* v. *Comm'n*, 1979 E.C.R. 461; Case T-228/97, *Irish Sugar* v. *Comm'n*, 1999 E.C.R. II-2975; and Case T-219/99 *British Airways* v. *Comm'n*, 2003 E.C.R. II-5925. In the United States, discount and rebate scheme programs can violate Section 2 of the Sherman Act. See *LePage's Inc.* v. *3M*, 324 F.3d 141, 157 (3d Cir. 2003); *Cascade Health Sols.* v. *PeaceHealth*, 502 F.3d 895, 905 (9th Cir. 2007); *Eisai Inc.* v. *Sanofi-Aventis U.S.*, Civil Action No. 08-4168, 2014 WL 1343254 (D.N.J. Mar. 28, 2014).

[34] Article 102(a) of the Treaty on the Functioning of the European Union (TFEU) refers to the imposition of unfair purchase or selling prices as well as other unfair trading conditions. Consolidated Version of the Treaty on the Functioning of the European Union art. 102(a), 2008 O.J. C. 115/47. See Case COMP/38.636, Rambus Inc., 2010 O.J. C 30 (the Commission had to deal with potentially abusive royalties for the use of patents).

Such abuses could be created by the creation of a dual blockchain environment, one for those who pay the most and one for those who pay less and whose transactions may lag behind as a result.

services in exchange for preferential treatment[35] or when one blockchain imposes unfavorable measures on another blockchain. In the BlockJobs example, users who are unwilling to pay to gain visibility will face unfair conditions such as preventing them reading information on the blockchain, forbidding them from proposing news transactions on the blockchain or keeping them from validating blocks. However, because blockchain is still evolving rapidly, there is little use in focusing too much attention on exploitative abuses. The dynamism of the blockchain environment will likely correct these abuses themselves. This type of abuse is nonetheless possible and will undoubtedly be litigated.

2.4. Discriminatory Abuses

Discriminatory abuses occur when parties apply "dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage" [O'Donoghue R., Padilla J., 2013: 795][36]. These abuses are practiced in various ways, although price discrimination is the most common[37]. According to Judge Richard Posner, "price discrimination is a term that economists use to describe the practice of selling the same product to different customers at different prices even though the cost of sales is the same to each of them. More precisely, it is selling at a price or prices such that the ratio of price to marginal costs is different in different sales" [Posner R., 2001: 79–80].

[35] Østbye P. The adequacy of competition policy for cryptocurrency markets. Aug. 24, 2017. Available at: https://www.google.com/search?ei=aRn9XJ7QLoKwrgTI1KPgCw&q=%C3%98stbye+P.+The+Adequacy+of+Competition+Policy+for+Cryptocurrency+Markets+%28Aug.+24%2C+2017%29%2C&oq=%C3%98stbye+P.+The+Adequacy+of+Competition+Policy+for+Cryptocurrency+Markets+%28Aug.+24%2C+2017%29%2C&gs_l=psy-ab.3...42761.43832..44723...1.0..0.86.86.1.....0....1j2..gws-wiz.....6..35i39.021KJ8SPffc (accessed: 17.05.2019)

[36] See TFEU Art. 102(c) and 2008 O.J. C. 115/47.

[37] In European judicial history, there are few cases in which price discrimination alone was found abusive. See Case T-301/04, *Clearstream Banking AG* v. Comm'n, 2009 E.C.R. 317 (referring to anticompetitive foreclosure when an 'as efficient competitor' cannot compete effectively with the price of the dominant undertaking); see also C209/10, *Post Danmark A/S* v. *Konkurrenceråd-det*, 2012 E.C.R. 172, (ECJ clarifying that where prices are below average total costs while being above average incremental costs, a finding of abuse requires a demonstration of actual or likely exclusionary effects). In the United States, price discrimination by a monopolist violates Section 2 of the Sherman Act only to the extent that it is predatory or otherwise excludes competitors from the relevant market. See *Blue Cross & Blue Shield United of Wis*. v. *Marshfield Clinic*, 65 F.3d 1406, 1413 (7th Cir. 1995). Price discrimination may also violate the Robinson-Putman Act. See *Brooke Group Ltd*. v. *Brown & Williamson Tobacco Corp*., 509 U.S. 209, 220 (1993).

Because price discrimination involves favoring certain customers over others, it generally occurs in two ways: charging different customers different prices for the same product, or charging only some customers the same price for different products.

Because of the "visible effect"[38] of public blockchains, occurrences of price discrimination will be limited. However, within private blockchains users may encounter discriminatory terms because the application of different terms to different users is an effective way to urge users to join and use a blockchain. Discriminatory pricing can incentivize some users to stay active on the blockchain by offering lower prices, thus creating a potential discrimination claim for others. Accordingly, discriminatory abuses are more likely to happen on private blockchains. In the BlockJobs example, Y may initiate discriminatory terms to thank a user for a commercial advantage granted in another market. Once again, private blockchains will be at the center of focus.

Conclusion

This paper has outlined several anticompetitive practices. Most of the usual antitrust instruments will be ineffective against public blockchains[39] because antitrust law does not provide complete answers to three questions: how are anticompetitive practices committed on public "permission-less" blockchains to be detected; how is the economic operator responsible for these practices to be identified; and, finally, how are they to be remedied in the future. While the perpetrator of an anticompetitive practice on a blockchain can sometimes be identified, the effectiveness of sanctions and remedies may be hindered by the immutability of the blockchain[40].

The situation is different for private permissioned blockchains. On this type of blockchain, antitrust issues such as refusal to deal, margin squeezing or predatory pricing most often when an interested competitor is refused access. Although there may be legitimate business justifications to exclude a rival, adhering to several best practices will minimize antitrust risk. The reasons for membership criteria should be well documented and well defined,

[38] See note 24.

[39] *May T.* The Crypto Anarchist Manifesto. Available at: https://www.activism.net/cypherpunk/crypto-anarchy.html (accessed: 17.05.2019)

[40] Guegan *D.* Op. cit.

and they should point to procompetitive justifications. Criteria should also not be so narrowly defined that they could be construed as purposely excluding a certain competitor or set of competitors. When applying membership criteria, owners of the blockchain should not treat similarly situated competitors differently. Reasons for expulsion should be defined and known to all members. Finally, reasons for the removal of any member should be well documented and fall within the established criteria for expulsion outlined at the formation of the blockchain.

Another competition concern linked to the use of a private blockchain pertains to the type of consensus mechanism it opts for. An owner, operator or its designee that serves as the membership "gatekeeper" may have the ability to control how data disputes are resolved. It also may restrict which participants have the right to read, edit or fix discrepancies. These procedural rules potentially allow exclusionary practices to occur within the blockchain. The owner, along with the designated participants, may agree to disadvantage certain competitors.

By resolving discrepancies using a pre-set, objective consensus mechanism, such as proof of work, no single participant can control how a discrepancy is resolved. This reduces the likelihood that discrepancies will raise competitive issues, for example, based on favoritism or as a result of collusion among rival members. If a different system must be deployed, discrete parameters should be established explaining how the designated participants must resolve the discrepancy. Such a system could include, for example, having discrepancies or disputes resolved by a rotating, random set of participants[41].

Another challenge to overseeing competition in the use of blockchain lies in the enforcement by centralized regulators, such as the US Department of Justice, the US Federal Trade Commission or the European Commission, of the vertically designed rules and concepts of antitrust law to a technology built around the desire for decentralization [Werbach K., 2018: 487]. Hence, the need to find new ways of decentralizing antitrust law and antitrust authorities [Freedman M., 1962: 202], through the design [Cuccuru P., 2017: 179] and the implementation of new governance models using blockchain [Abramowicz M.,: 2016: 359,420].

[41] Thomas R. Op. cit., p.13.

References

Abramowicz M. (2016) Cryptocurrency-Based Law. *Arizona Law Review*, no 2, pp. 359, 420.

Bork R. (1978) *The Antitrust Paradox: A Policy at War with Itself*. New York: Basic Books, p. 462.

Bradley R., Summers L. (1990) On The Origins of the Sherman Act. *The Cato Journal*, no 3, pp. 737, 740.

Champagne P. (2014) *The book of Satoshi: The collected writings of Bitcoin creator Satoshi Nakamoto*. Plano: Publishing LLC, p. 136.

Cuccuru P. (2017) Beyond Bitcoin: An Early Overview on Smart Contracts. *International Journal of Law & Information Technology*, 2017, no 3, p. 179.

Dannen C. (2017) *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*. New York: Apress, p. 185.

De Filippi P., Wright A. (2018) *Blockchain and the Law: the Rule of Code.* Boston: Harvard University Press, p. 209.

Devlin A. & Jacobs M. (2012) Anticompetitive Innovation and the Quality of Invention. *Berkeley Technology Law Journal,* no 1, pp. 1–53.

Economides N., Lianos I. (2010) Elusive Antitrust Standard on Bundling in Europe and in the United States in the Aftermath of the Microsoft Cases. *Antitrust Law Journal*, vol. 76, p. 483.

Ernst D. (1990) The New Antitrust History. *New York Law School Law Review*, no 35, p. 879.

Freedman M. (1962) *Capitalism and Freedom*. Chicago: University of Chicago Press, p. 202.

Hawk B (2018) English Competition Law before 1900, *The Antitrust Bulletin,* no 1, p. 19.

Huberman G. (2017) Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System, *Columbia Business School Research Paper*, no 17–92, p. 2.

Kaiser H. (2011) Are “Closed Systems” an Antitrust Problem? *Competition Policy International,* no 7, pp. 91, 102–103.

Kreps D., Wilson R. (1982) Reputation and imperfect information. *Journal of Economic Theory*, no 2, p. 253–279.

Markovits R. (2014) Economics and the Interpretation and Application of U.S. and E.U. Antitrust. *The Antitrust Bulletin*, no 59, pp. 3, 19.

O’Donoghue R., Padilla J. (2013) *The Law and Economics of Article 102 TFEU*. Oxford: Hart, p. 795.

Popper N. (2016) Digital. *Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money.* New York: Harper, p. 412.

Posner R. (2001) *Antitrust Law*. Chicago: University of Chicago Press. p. 304.

Posner E., Weyl G. (2018) *Radical Markets: Uprooting Capitalism and Democracy for a Just Society.* Princeton: Princeton University Press, p. 368.

Raskin M. (2017) The Law and Legality of Smart Contracts. *Georgetown Law Technology Review,* no 1, p. 305.

Raval S. (2016) *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology.* Sebastopol (Cal.): O'Reilly Media, p. 106.

Rochet J.-C., Tirole J. (2003) Platform Competition in Two-Sided Markets*. Journal of the European Economic Association,* no 4, p. 990.

Schrepel T. (2018) Predatory Innovation: The Definite Need for Legal Recognition. *Science & Technology Law Review,* no 21, p. 22.

Schrepel T. (2018) Antitrust conversations with Nobel laureates. *Concurrentialiste Review,* no 1, p. 15.

Schrepel T. (2019) Collusion by Blockchain and Smart Contracts. *Harvard Journal of Law & Technology,* no 1, p. 118.

Swan M. (2015) *Blockchain: Blueprint for a New Economy.* Sebastopol (Cal.): O'Reilly Media, p. 131.

Tapscott D., Tapscott A. (2016) *A Blockchain Revolution: How the Technology behind Bitcoin is Changing Money, Business and the World.* New York: Random House, p. 358.

Tsu S. (2017) *The Art of War*. London: Macmillan, p. 152.

Vigna P., Casey J. (2018) *The Truth Machine: the Blockchain and the Future of Everything*. New York: St. Martin's Press, p. 302.

Walch A. (2017) The Path of the Blockchain Lexicon (and the Law). *Review of Banking & Financial Law*, no 36, p. 713.

Werbach K. (2018) *The Blockchain and the New Architecture of Trust.* Cambridge (Mass.): MIT Press, p. 344.

Werbach K. (2018) Trust, but Verify: Why the Blockchain Needs the Law. *Berkeley Technology Law Journal,* no 33, p. 487.