



BALTIC JOURNAL OF LAW & POLITICS

A Journal of Vytautas Magnus University

VOLUME 13, NUMBER 1 (2020)

ISSN 2029-0454



Cit.: *Baltic Journal of Law & Politics* 13:1 (2020): 81-107

<https://content.sciencedirect.com/view/journals/bjlp/bjlp-overview.xml>

DOI: 10.2478/bjlp-2020-0004

POTENTIAL LEGAL CHALLENGES FOR BLOCKCHAIN TECHNOLOGY IN COMPETITION LAW

Christophe S. Hutchinson

Senior Lecturer

**Financial University under the Government of the Russian Federation,
Department of Legal Regulation of Economic Activities (Russian Federation)**

Contact information

Address: Leningradsky Prospekt, 49, Moscow, Russian Federation, 125993

Phone: + 7916 658 44 22

E-mail address: sam_hutch2004@yahoo.fr, KSYUchinson@fa.ru

Maria A. Egorova

Doctor of Law; Professor; Head of the Department

**Kutafin Moscow State Law University, International Cooperation Department
(Russian Federation)**

Contact information

Address: Sadovaya-Kudrinskaya, 9, Moscow, Russian Federation, 125993

Phone: +7 925 577 87 55

E-mail address: MAEGOROVA@msal.ru

Received: March 5, 2020; reviews: 2; accepted: July 16, 2020.

ABSTRACT

Since decentralized organizations such as blockchain are not recognized as legal persons, questions arise regarding the ability to detect anti-competitive practices and their perpetrators. Under certain circumstances, if a competitor is unreasonably refused in access to technology, it may well be interpreted as creating an obstacle to his/her entry into the market, which may constitute a violation of the legislation of a country on the protection of

economic competition. The exchange of information between players of the same market can present antitrust risks if it helps to fix prices for their products/services or to establish other forms of coordination between such players. The purpose of this study is to provide a description of current EU anticompetitive practices in the field of blockchain-technologies application, as well as to identify challenges in the EU antitrust law related to the emergence of blockchain. This article highlights the challenges blockchain poses for analyzing unilateral anti-competitive practices. This study suggests that EU competition law has a lack of operational and measurement tools to map competitive interactions taking place outside the relevant market, which could lead to rather short-sighted competition law enforcement focusing only on horizontal competition restrictions on relevant markets. The relevance of the topic is associated with the fact that the increased popularity of the use of blockchain technology requires an answer to the question of its legal nature and inclusion in the legal field in order to balance the interests of all parties to economic and legal relations.

KEYWORDS

Abuse of dominance, antitrust, cryptology, distributed ledger, exclusionary abuse, exploitative abuse, network protocol

INTRODUCTION

Blockchain is a general-purpose technology that threatens to disrupt markets and institutions around the world. While the internet allows the publication and digital transfer of information, blockchain makes it possible to identify the ownership of the assets, make them unique and traceable, facilitate digital transfer and, consequently, the exchanges of assets, by offering trust in the transaction and reducing uncertainties (through the use of a self-executing code that is trustworthy).

The World Economic Forum predicts that 10% of the world's gross domestic product will be stored on blockchain by 2027.¹ Blockchain's attractiveness lies in its ability to drastically reduce the transactional costs² required to create trust between parties through the recourse to intermediaries such as banks, brokers, governments, internet platforms, law firms etc.³ It can indeed facilitate contracting and mitigate widespread contractual inadequacies⁴ by creating a world in which computers fill the gaps of contracts.

While facilitating trade, blockchain gives rise to many legal challenges with significant 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 defined as an antitrust law, using the American terminology that emerged as a reaction to the misuse of the trust instrument.⁵ On the other hand, blockchain technology eliminates the need for a fiduciary, that is, a person who creates trust, because it works automatically, without any physical or artificial person.

This article aims to highlight the challenges that blockchain presents for the analysis of unilateral anti-competitive practices.⁶ The article is organized in two parts. The first part describes how block chain functions. The article then argues that, because blockchain is anonymous, immutable and decentralized, questions arise about the ability to detect anti-competitive practices and their authors. There

¹ World Economic Forum, "Deep Shift: Technology Tipping Points and Societal Impact" (2015) // <https://www.weforum.org/reports/deep-shift-technology-tipping-points-and-societal-impact>.

² Russ. Roberts, and Jim Epstein, "Jim Epstein on Bitcoin, the Blockchain, and Freedom in Latin America," *Econ Talk* (2017) // <http://www.econtalk.org/jim-epstein-on-bitcoin-the-blockchain-and-freedom-in-latin-america/>.

³ Alan Penz-Sharp, "Blockchain for Business: Ready or Not, Here it Comes," *CMSWire* (2017) // <https://www.cmswire.com/information-management/blockchain-for-business-ready-or-not-here-it-comes>.

⁴ Lin Cong and Zhiguo He, "Blockchain Disruption and Smart Contracts," *The Review of Financial Studies* 32 (2018): 1754.

⁵ See The legislative history of the Federal antitrust laws and related statutes 10–13 (1978); Robert Bradley, "On the Origins of the Sherman Antitrust Act," *Cato Journal* 9 (1990): 737; Kiran Desai, *Blockchain and competition law* (London: Ernest & Young Law Alert, 2018), 52 // [https://www.ey.com/Publication/vwLUAssets/ey-blockchain-and-competition-law/\\$FILE/ey-blockchain-and-competition-law.pdf](https://www.ey.com/Publication/vwLUAssets/ey-blockchain-and-competition-law/$FILE/ey-blockchain-and-competition-law.pdf); Eric Posner and Glen Weyl, *Radical Markets: uprooting capitalism and democracy for a just society* (Princeton: Princeton University Press, 2018), 33.

⁶ We exclude cartels from this study in order to keep this article to a reasonable length. Many of the developments of this article can nonetheless be applied to cartels analysis. For a specific study of blockchain challenges created for collusive agreements.

arises from the ramified nature of the blockchain a question about the efficiency of current competition legislation, which relies on centralized legal structures and enforcement, incompatible with the nature of blockchain.

This current study is based on European Union legislation (Treaty on the Functioning of the European Union) as well as the EU authorities' law enforcement practices (judgments of the European Court of Justice in the case C209/10, *Post Danmark A/S v. Konkurrencerådet*, 2012 E.C.R. 172, case T-301/04, *Clearstream Banking AG v. Comm'n*, 2009 E.C.R. 317). In this case, one should pay attention to the fact that the technology itself has been created without any reservations about jurisdiction. Using the method of political and legal analysis, this study aims to provide a holistic description of modern anti-competitive practices in the field of blockchain application. The study considers the current state of the EU antitrust regulatory framework in the context of its applicability to legal relationships arising from the emergence of blockchain technologies. At the same time, attention is given to consideration of anti-competitive practices in the field of blockchain application that fall under the EU antitrust legislation. In order to provide a comprehensive understanding of the reasons for the difficulties in legislative regulation of legal relations in the field of applicability of blockchain technology for antitrust law, the study also focuses on the issues of the technological component and evolution of blockchain.

1. THE FUNCTIONING OF BLOCKCHAIN

This section focuses solely on the fundamentals of blockchain operation, 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. It also explores the differences between blockchain 1.0, 2.0 and 3.0 to show how blockchain is used today and what direction it can take.

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 trust⁷ between people who have no reason to trust one another. Blockchain combines the following

⁷ Satoshi Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Bitcoin* (2008) // <https://bitcoin.org/bitcoin.pdf>.

three technologies: distributed ledger,⁸ cryptology and network protocol. Distributed ledger enables the storing of the same info in different places.⁹

Blockchain has numerous advantages: first it is decentralized. The network exists across a series of nodes formed by the computers that store the blockchain info and contribute also 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"¹⁰ to the transaction being carried on the network. The consequence of decentralization is no single participant controls the information on the blockchain.

A second gain of blockchain is that it is 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 it at any one given time.¹¹

Third it is anonymous,¹² 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.¹³

Lastly, Blockchain is immutable¹⁴ since once information is stored on a block; it cannot be tampered by individual participants, unless the whole network agrees to such a change.

Despite all the advantages that blockchain technology can bring and already brings, there is a general background of distrust in society, and sometimes even an unreasonable bias towards it. At the same time, in Europe and around the world, blockchain is perceived not only as a tool for working with cryptocurrency or purely financial technology but as a mechanism applicable in almost all daily activities.¹⁵ The interest in blockchain technologies at both the private and state levels is growing rapidly (See Pic. 1: Worldwide spending on blockchain solutions).

Blockchain technology is closely related to and in a certain sense comes from the P2P (peer-to-peer) technology preceding it. P2P information systems are systems in which there is no separation between clients and servers, no central

⁸ Siraj Raval, *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology* (Sebastopol: O'Reilly Media, 2016), 35.

⁹ Posner and Weyl, *supra* note 5, 33.

¹⁰ Ross Mauri, "Three Features of Blockchain that Help Prevent Fraud," *IBM* (2017) // <https://www.ibm.com/blogs/blockchain/2017/09/three-features-of-blockchain-that-help-prevent-fraud>.

¹¹ Most of the data placed 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.

¹² Phil Champagne, *The book of Satoshi: The collected writings of Bitcoin creator Satoshi Nakamoto* (USA: e53 Publishing, 2014), 51.

¹³ Don Tapscott and Alex Tapscott, *A Blockchain Revolution: how the technology behind Bitcoin is changing money, business and the world* (New York: Penguin Random House, 2016), 38.

¹⁴ Angela Walch, "The Path of the Blockchain Lexicon (and the Law)," *Review of Banking & Financial Law* 36 (2017): 713.

¹⁵ IDC Trackers, "Worldwide Blockchain Spending Guide" // https://www.idc.com/tracker/showproductinfo.jsp?prod_id=1842.

administrator or any analogue of it. The anonymity of the P2P system and the absence in it of a central administrator performing supervisory functions naturally raise concerns among monetary regulators. Such systems initially excluded the participation of the national financial regulator, the presence of monetary policy, and the central government, which was a completely peer-to-peer network for storing and transferring value.¹⁶

In light of the evolution of the blockchain, its interconnection with the technology of public key infrastructure (PKI) should be noted. This technology has been created to uniquely and correctly identify the identities of users, devices and services. At the same time, since the entire infrastructure of public keys rests almost entirely on trust in the authentication system, the compromise of just one secret key practically "nullifies" the entire infrastructure, which in some cases takes millions of dollars to build. It is likely that over time all PKI management problems will be "inherited" by the blockchain. When digital identifiers do come to replace paper documents and passwords for logging into systems, they will likely be based on distributed registries similar to modern blockchains.¹⁷

1.2. PUBLIC VS. PRIVATE BLOCKCHAIN

There are several types of blockchain. The difference comes down to whether the info stored on the blockchain is public or private and whether potential nodes and users on the network need permission to join or not.

A public blockchain¹⁸ is open to all. To become a node on that network, each participant needs to set up its computer by implementing the governing protocol. He can remain pseudonymous behind a unique user identifier within the network. The ledger tracks each participant by its identifier. The ledger is transaction-based, and it notes the prior transaction history. This information can be used to assess if 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 preset rules, a "consensus mechanism," to decide which record should prevail.

¹⁶ Sunghyuck Hong, "P2P networking based internet of things (IoT) sensor node authentication by Blockchain," *Peer-to-Peer Netw.* 13 (2020): 579.

¹⁷ Maurizio Talamo, Franco Arcieri, Andrea Dimitri, and Christian H. Schunck, "A Blockchain based PKI Validation System based on Rare Events Management," *Future Internet* 12 (2020): 40.

¹⁸ Public blockchains are also called "permission-less" or "open" blockchains.

For example, on the *Bitcoin* blockchain, the party 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 correctly, 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 on how to resolve them.¹⁹

A public permissioned blockchain is a system where the information is public but the writing of new information or the verification of a new transaction requires the permission from a central authority. Such is the case, for instance, of a blockchain on 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 enter 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 a permissioned one since changes of property require permission from a State. The Swedish government, for instance, is currently looking at public permissioned blockchain as a way to collect land tax more efficiently, since it is virtually up-dated all the time and it enables to link the land registry blockchain to GPS references.²⁰

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 info can only be used by the members of the network because it's private. The central authority doesn't need to be just one entity. A group of entities often occurs on a private blockchain. This kind of permissioned blockchain has been used by, for example, the banking system for interbank transactions, clearing or settlement or transferring account between insurance providers. In such a 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, as the holder of an equity or

¹⁹ Ryan Thomas, "Blockchains and Antitrust: new technology, same old risks," *JonesDay One Firm Worldwide Whitepaper* (2018) // <https://www.jonesday.com/blockchains-and-antitrust-new-technology-same-old-risks-08-02-2018/>.

²⁰ The World Bank, "Blockchain or distributed ledger technology," *The World Bank Group* (2018) // <http://documents1.worldbank.org/curated/pt/260121548673898731/pdf/134063-WP-121278-2nd-edition-IFC-EMCompass-Blockchain-Report-PUBLIC.pdf>

security, will only have access to his particular part of the chain which is his account on the chain.

1.3. CONSENSUS MECHANISM AND GOVERNANCE

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

Several major blockchains (*Bitcoin* and *Ethereum*, for example) currently use a form of consensus based on proof of work, in which some users, here called miners, rush to solve a cryptographic puzzle in order to be chosen to verify the integrity of transactions.²¹ The first to solve it is rewarded by receiving a transaction fee. Many public blockchains are currently working on developing proof of stake,²² a consensus achieved by cryptoeconomics and game theory.²³

With private blockchain, however, there is generally no mining, no proof of work, and no remuneration.²⁴ The benefits of private blockchain come from its valuation and applicability.²⁵ Uses of private blockchain include (1) serving as a transfer value (currency, securities, votes, industrial patents, Internet of Things (IoT), stocks, bonds),²⁶ (2) serving as a register to verify the exchange of products and assets;²⁷ and (3) serving as a smart contract by enabling an automatic program to insert terms and conditions.²⁸

Whoever controls the consensus—also known as the consensus mechanism—controls the governance of the blockchain.²⁹ The consensus operates and communicates between network nodes. For instance, *Dash*, a crypto-currency,³⁰ 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 Masternode, have more power within the

²¹ Paul Vigna and Michael Casey, *The Truth Machine: the Blockchain and the Future of Everything* (New York: St. Martin's Press, 2018), 37.

²² Vlad Zamfir, "Introducing Casper 'The Friendly Ghost'," *Ethereum Blog* (2015) // <https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost>.

²³ For instance, *Ethereum* is said to intend to migrate to proof of stake.

²⁴ Some private blockchains use proof of work and are moving to proof of stake.

²⁵ On the contrary, the main incentive to use public blockchains is that using it brings value, and value brings profitability.

²⁶ Dominique Guegan, "Public Blockchain Versus Private Blockchain," *Documents de travail du Centre d'Economie de la Sorbonne* 1 (2017): 17020 // <https://halshs.archives-ouvertes.fr/halshs-01524440/document>.

²⁷ *Ibid.*

²⁸ Pierluigi Cuccuru, "Beyond Bitcoin: An Early Overview on Smart Contracts," *International Journal of Law and Information Technology* 25 (2017): 179.

²⁹ Gur Huberman, Jacob Leshno, and Ciamac Moallemi, "An Economic Analysis of the Bitcoin Payment System," *Columbia Business School Research Paper* 2 (2017): 17.

³⁰ See DASH // <https://www.dash.org>.

community. A blockchain's ability to implement anti-competitive strategies will vary depending on the governance system of the blockchain.

1.4. FROM BLOCKCHAIN 1.0 TO BLOCKCHAIN 3.0

Antitrust concerns about the blockchain platforms and the software operating on it entail different types of anti-competitive practices³¹: those that are committed via the blockchain itself as a platform and those that are committed via the applications working on the blockchain.

Not all blockchains allow software ("layer 2") to run on the *root blockchain* ("layer 1"), but most do. *Ethereum*, for example, is a root blockchain that allows any type of software layer. In fact, *Ethereum* has been specifically designed to allow users to create "smart contracts" or agreements between accounts to automatically transfer tokens when certain conditions are met.³² Anyone can download a program on this platform and leave it to self-execute securely.³³

These blockchain applications can be distinguished by three generations of blockchain. The first, blockchain 1.0, is similar to a currency and includes "cash, such as currency transfer, remittance and digital payment systems".³⁴ The second, blockchain 2.0, is a contract comprising "stocks, bonds, futures, loans, mortgages, securities, smart properties and smart contracts"; this category includes all blockchains allowing applications that enable financial activities.³⁵ Finally, blockchain 3.0 includes all "applications other than finance and markets, particularly in the areas of government, health, science, literacy, culture and the arts".³⁶

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

2. COMPETITION CHALLENGES

The blockchain sets two main types of competition challenges: it complicates both the characterization of dominant market positions and the attribution of responsibility for anti-competitive practices. This is all the more worrying as anti-competitive practices are expected on blockchain, as demonstrated below by analyzing how and why monopolization practices could be implemented on it.

³¹ Peder Østbye, "The Case for a 21 Million Bitcoin Conspiracy," *Journal of Financial Transformation* 48 (2018): 88.

³² Chris Dannen, *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners* (New York: Apress, 2017), 63.

³³ Tapscott, *supra* note 13, 38.

³⁴ Melanie Swan, *Blockchain: Blueprint for a new economy* (Sebastopol: O'Reilly Media, 2015), 29.

³⁵ *Ibid.*

³⁶ *Ibid.*

Virtually, blockchain technology itself is neither pro nor anti-competitive in nature. At the moment and in the foreseeable future, it is unlikely that any particular blockchain will take a dominant position. However, a likely situation for the alleged abuse of the dominant position will be a rejection of the transaction (not allowing the subject to join the blockchain community), such as, for example, in a situation where among European banks there is a blockchain for interbank payments. There may be another way, namely, clearing interbank payments, which is valid, but slow and expensive in comparison. If a new bank would like to open a business in Europe, membership in the blockchain may be necessary if it intends to become competitive. If a new bank is denied access or membership for biased reasons or at a cost that is not objective and reasonable, this may constitute an abuse of dominance.³⁷

2.1. CHARACTERIZATION OF THE DOMINANT POSITION IN THE RELEVANT MARKET

The European Commission (EC) has said that the almost unbounded list of possible use cases for Distributed Ledger Technology (DLT) makes it both very promising and challenging, and expressed its support for blockchain and DLT. However, many European institutions still believe that the technology is at an early stage of development and therefore it is too early to regulate it. They reasonably see the risk that early regulation could limit its future development and potential. Moreover, regulation too early may not regulate the relationship properly and reduce the risks associated with the use of blockchain technology³⁸.

The European Central Bank (ECB) is closely monitoring innovative fintech solutions, including blockchain technologies. The ECB recognizes the potential benefits of blockchain technologies and has even created a dedicated Distributed Ledger Technology working group that brings together market experts on financial innovation and cybersecurity³⁹.

Defining relevant markets is a tool to define the boundaries of competition between companies taking into account material and geographical dimensions. The definition of such markets on digital markets can be complex.

Blockchain raises important questions about what a dominant position is. Because decentralized organizations like blockchain are not recognized as legal

³⁷ Desal, *supra* note 5, 52.

³⁸ Jurgita Miseviciute, "Blockchain and virtual currency regulation in the EU," *Journal of Investment Compliance* 19 (2018): 33.

³⁹ *Ibid.*

⁴⁰ European Central Bank, "Why does the ECB have a stake in market infrastructure?" (2016) // <https://www.ecb.europa.eu/pub/annual/special-features/2016/html/index.en.html>.

persons,⁴¹ many issues arise, such as: "Can a non-entity hold a dominant position?" Can blockchain create a "monopoly without a monopolist?"⁴² Finally, if the blockchain is dominant, which users and/or entities hold that dominant position?

Depending on the way in which a dominant position is characterized, liability will be attributed in different ways, given that an entity holding a dominant position is fully liable for the practices implemented within it. The same goes for blockchains: the way in which dominance is characterized will determine the extent of liability.

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

The first theory of liability would be to consider that each blockchain, as a general ledger on which transactions are recorded, would constitute a relevant market. 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 trying to prevent the implementation of anti-competitive practices by a fraction of the users. This assumption, again, comes from the technological essence and purpose of the blockchain that the concept of blockchain has originated in the technical environment, without regard to any legal aspects. Considering blockchain technology from such a position would completely level its essence and technical features. Retaining such a market definition would significantly reduce the incentive to use blockchains, as unintentional users could be held liable for practices performed by third parties unknown to them. As such, this first way of defining dominant positions should be rejected.

A second theory would consist in determining market power based on the type of applications (products and services) that run on the blockchain as a layer.⁴³ The type of blockchain (1.0, 2.0 or 3.0) which constitutes different layers of smart contracts⁴⁴ will then be at the center of the market definition in which the two-sided nature⁴⁵ of the market will be taken into account by analyzing the functions

⁴¹ Primavera De Filippi, *Blockchain and the law: the Rule of Code* (Boston: Harvard University Press, 2018), 18.

⁴² Huberman, *supra* note 29: 17.

⁴³ A distinction would be further 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 blockchain can be integrated into a wider market—as it 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 will have to be evaluated.

⁴⁴ Swan, *supra* note 34, 29.

⁴⁵ Jean-Charles Rochet, and Jean Tirole, "Platform Competition in Two-Sided Markets," *Journal of the European Economic Association* 1 (2003): 990.

of the 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, the blockchain's market power would be assessed in comparison with other digital products or services and, potentially, non-digital alternatives. As a result, blockchain power would be evaluated the same way as online sales can be integrated into the general sales market (including physical sales).⁴⁶

Such a characterization of a dominant position would make it possible to retain liability only for users who offer, exploit or use a dominant application that has engaged in anti-competitive 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 anti-competitive practice.

However, the question remains as to which elements to take into account in order to evaluate the market power between blockchains running the same type of applications: the number of users, the number of transactions recorded, the number of blocks; revenues, etc.?

In the *Google* decision, the ECJ noted that the European Commission had used market shares by volume as a proxy for several reasons. "First, market shares cannot be calculated because general search services are provided free of charge to the user. Secondly, despite its best efforts, the Commission has been unable to obtain accurate and verifiable Revenue per Search ("RPS") values on the main general search services. Third, advertisers examine usage shares to decide where to place their search ads."⁴⁷

With regard to the geographical dimension of relevant markets, it should be emphasized that, although the language used on blockchain is universal, some applications may be focused on a local market, while others may compete at world level. Here, only a case-by-case analysis is possible.

In short, assessing the market power of a blockchain network creates new challenges, one of which is the lack of central power needed to ask the majority of the blockchain users to adopt changes, which significantly reduces the idea of "power".⁴⁸

2.2. THE ABUSE OF DOMINANCE

This section focuses on the different types of unilateral practices (exploitation, exclusion and discrimination) that may occur with blockchains. Before analyzing

⁴⁶ See, for instance, *Case Google Shopping*, No. 39740, 2017 E.C.R. 145, in which the market definition was established by comprising the totality of interchangeable products or services.

⁴⁷ *Ibid.*

⁴⁸ Seoung Kim, "Ethereum Upgrades as Hard Forks Activate on Blockchain," *Coindesk* (2019)

these unilateral practices in greater detail, two common trends are worth highlighting.

All information and transactions recorded on public blockchains are, up to a certain extent, visible by all. With regard to private blockchains, transactions are only visible to its users if they are designed in that way.⁴⁹ As a result, the number of anti-competitive practices may be lower on public blockchains than in other technology markets, precisely because public channel chains create greater transparency between users.⁵⁰

Therefore, it is to be expected that, since transactions can be viewed by all blockchain users, the inherent transparency tends to prevent the implementation of anti-competitive practices, thereby reducing their number. But vigilance is required, because unilateral practices will not entirely disappear because of blockchain's so called "opacity effect". On blockchain all transactions are encrypted⁵¹ and the identity of blockchain users is protected by anonymity. As a consequence, a transaction may be visible, but the nature and the goal of the transaction are unknown to outsiders, which makes the interaction between users more opaque. This "opacity effect" is even stronger on private blockchains where the content of the blockchain is kept secret from outsiders.

To demonstrate which unilateral practices might be implemented on blockchain, let us assume the hypothetical situation of the company Y 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 it can choose the users who may access the blockchain, which operations the users can perform on it and which protocol governs 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 of its blockchain. *BlockJobs* allows users to post and /or apply for jobs. At each stage of the recruitment process, from the first interview to the acceptance or rejection 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 users looking for candidates pay with tokens. After a while, this application is very successful 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 anti-competitive strategy.

⁴⁹ 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.

⁵⁰ Sun Tsu, *The Art of War* (London: Macmillan, 2017), 58.

⁵¹ Kevin Werbach, "Trust, but Verify: Why the Blockchain Needs the Law," *Berkeley Technology Law Journal* 33 (2018): 487.

With regard to the issue of determining the economic and legal component of anti-competitive practice, it can be relatively simple to determine whether the activity in question is an 'undertaking'. In the case of collusion (managed or supported by DLT technology) everything would depend on the activity of the owners of the nodes (for example, any active electronic device connected to the Internet and getting rid of the IP address) maintaining the network by maintaining a copy of the blockchain and ultimately, transaction processing. To the extent that node owners voluntarily provide their computing resources for storing and verifying transactions, receiving a transaction fee or reward in their own token of a particular blockchain, they are engaged in economic activity⁵².

The definition of a legal entity that will be held liable for violating competition law presents great difficulties due to the decentralized nature of the blockchain. Although the concept of "entity" is less important in determining the existence of "economic activity", given the functional approach used in EU competition law it becomes critical when it comes to determining the liability under Article 101 TFEU of two organizations because they entered into an illegal agreement or concerted action, making the illegal conduct and the related issue of remedies / sanctions liable, and determining the market share of the company involved in a competition law violation, such as in the context of merger control or in the context of abuse of dominance.⁵³

2.2.1. EXCLUSIONARY ABUSE

Exclusionary abusive practices include the refusal to deal, tie-in sales, predatory pricing, margin squeeze or exclusive dealing and rebates.

Refusal to deal

Article 102 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 ECJ has found antitrust liability when a monopolist refused to sell a product to a competitor that it made available to others.⁵⁴

Refusal to deal is a common practice outside⁵⁵ blockchains, but it should be rarer with blockchains, at least when it comes to public blockchains. A refusal to

⁵² Ioannis Lianos, "Blockchain Competition," *CLES Research Paper Series* 4/2018 (2018) // https://sci-hub.tw/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3257307.

⁵³ *Ibid.*

⁵⁴ Thomas, *supra* note 19.

⁵⁵ Privacy 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

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 necessarily possible. As a result, the refusal to deal can only be made possible by modifying the access rules themselves. Exclusionary strategies are therefore incompatible with the inherent nature of public blockchains and the blockchains that implement them will no longer be considered as “public” blockchains.

By way of contrast, the refusal to grant general access is an essential characteristic of private blockchains.⁵⁶ 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 be managed by different types of actors, depending on the governance choices. For instance a “(r)efusal 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”.⁵⁷ In order to illustrate a situation of refusal to deal (not allowing an entity to join a blockchain community), we shall imagine that a blockchain exists among European banks for interbank payments.⁵⁸ 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 for nonobjective reasons or on a cost basis that is not objective and reasonable, this might constitute an abuse⁵⁹ within the meaning of article 102 TFUE.

In case permissioned blockchain gains the status of an essential infrastructure and refusal to give access to it is not objectively justified, a gatekeepers’ exclusionary efforts also risk violating Art. 102 TFEU.⁶⁰

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.

⁵⁶ For a general overview on European refusal to sell, see Case *Oscar Bronner v. Mediaprint Zeitungs und Zeitschriftenverlag*, No. C-7/97, 1998 E.C.R. I-7796; Cases *European Night Servs. Ltd. (ENS) v. Commission*, No. T-374/94, T375/94, T-384/94, and T-388/94, 1998 E.C.R. II-3141; Case *Clearstream Banking AG v. Comm’n*, No. T-301/04, 2009 E.C.R. 317. In short, refusing to provide access to a facility is abusive if it is likely to eliminate all competition on the secondary market, if access is indispensable for entering the market in question, and if access is denied without any objective justification. For an overview of American refusal to deal, see Case *Verizon Comm. Inc. v. Law Offices of Curtis V. Trinko, LLP*, No. 540, 2004 U.S. 398, in which the court suggested that a refusal to deal motivated solely by a desire to eliminate competition, with no other purpose, might constitute illegal monopolization. To establish liability under the essential facilities doctrine, a plaintiff must show that the monopolist holds control over the essential facility, the plaintiff’s inability to duplicate the essential facility, the denial of use of the facility, and the feasibility of providing access to the facility.

⁵⁷ OECD, *Blockchain Technology and Competition Policy: Issues Paper by the Secretariat* (OECD, 2018) // [https://one.oecd.org/document/DAF/COMP/WD\(2018\)47/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf).

⁵⁸ By way of contrast, the refusal to grant access to the blockchain could be an abuse of dominant position if decided by one company, but it could also be a cartel if the blockchain is run by a consortium.

⁵⁹ Desal, *supra* note 5, 52.

⁶⁰ *Ibid.*

Tying/bundling

Tying is the practice of making the sale of a product (or service) conditional to additional sales or obligations.⁶¹ Tying may also involve the subjection of a contract to the acceptance of additional obligations unrelated to the original subject of the contract.⁶²

Tying is unlikely to occur in public blockchains. Indeed, this type of blockchain is freely accessible or usable. As a result, submitting it to the use of another product or blockchain is unlikely. On the other hand, private blockchains may, if created by for-profit corporations, have an interest in imposing tying or similar practices. Bundling effects may occur if an undertaking links the use of a blockchain (specialized, for instance, in the mining of a particular cryptocurrency's tokens) with ancillary services (e.g. digital wallet or exchange) offered outside the blockchain, on which the undertaking holds a dominant position.⁶³ Tie-in sales such as this one are therefore expected on private blockchains.⁶⁴

Predatory pricing

Another anti-competitive practice consists in driving a smaller competitors out of the market by systematically undercutting its prices.² On blockchain, pricing occurs mainly in the form of expensive transaction fees when a user submits a transaction to be recorded into the chain. Predatory pricing is very unlikely on public blockchains as it would only be possible if enough users could be convinced to change the governance structure to facilitate such a change.

The situation could be quite different for private blockchains if, for example, a large block validator or a mining pool set transaction fees below cost so as to exclude a rival cryptocurrency, or cross-subsidizes certain key merchants and suppliers in order to prevent a competing cryptocurrency from reaching efficient scale and, thus, profitably entering the market. These practices may be successful as they will not usually require the dominant undertaking to sacrifice profits; this usually acts as a disincentive for adopting exclusionary practices. In view of the

⁶¹ For an overview of tying, see *Case Microsoft Corp. v. Sun Microsystems, Inc., Comm'n Decision*, No. 3/37.792, Apr. 21, 2004. For American cases, see *Case Jefferson Parish Hosp. District No. 2 v. Hyde*, No. 466, 1984 U.S. 2, 1; *Case United States v. Microsoft Corp.*, No. 253, 2001 F.3d 34. Though the U.S. seemed to adopt the rule of reason after the *Case Illinois Tool Works Inc. v. Independent Ink, Inc.*, No. 547, 2006 U.S. 28, "the general per se rule for tying arrangements when market power is present very likely still survives," per Herbert J. Hovenkamp, "The Rule of Reason," *Florida Law Review* 70 (2018): 96. For more on bundling, see Nicholas Economides, and Ioannis Lianos, "Elusive Antitrust Standard on Bundling in Europe and in the United States in the Aftermath of the Microsoft Cases," *Antitrust law Journal* 76 (2010): 483-494.

⁶² For example, a blockchain application call Omnia asks for an Ethereum Wallet Address. See Omnia Round 2 (OM), Airdrop Alert.Com, accessible at <https://airdropalert.com/omnia-round-2-airdrop>.

⁶³ Peder Østbye, "The Adequacy of Competition Policy for Cryptocurrency Markets," *Social Science Research Network* (2017) // <https://www.competitionpolicyinternational.com/the-adequacy-of-competition-policy-for-cryptocurrency-markets/>

⁶⁴ It will still be necessary, however, to demonstrate the anticompetitive effect.

lower likelihood of successful entry, because of these exclusionary practices investors may be discouraged to participate in the ICOs launched by potential entrants, which, in view of the significance of this upfront method of attracting investment for blockchain projects, will certainly be sufficient to deter entry.⁶⁵ The predatory pricing test that takes into account average variable costs would then apply.

Margin squeeze

Another related practice occurs when a vertically integrated dominant firm operates on upstream and downstream markets and sets the upstream price high enough that companies can't compete sustainably in the downstream market.⁶⁶

By definition and by contrast, public blockchains are horizontal. It is therefore very unlikely that a margin squeeze will be applied to public blockchains. The case is different, however, for private blockchains. Because they enable revenue-generating applications while maintaining a financial interest on the platform layer, one can conceive that a strategy of margin compression could be implemented. This would require the dominant company (here the blockchain gatekeeper) to change the price it charges on the upstream market (i.e. the blockchain platform). In the development phase of blockchain, such a strategy seems unlikely, but it will have to be closely monitored in the coming years.

Exclusive dealing

Another practice which falls under the prohibition foreseen in article 102 TFEU consists in the requirement of a supplier with monopoly power to its customers to use its blockchain to complete transactions under the condition that they abandon the competitor's blockchain.⁶⁷ Such a condition may be included in the user agreement which is signed before using the blockchain.⁶⁸

⁶⁵ Østbye, *supra* note 63.

⁶⁶ Comm'n of The European Communities, "Guidance on the Commission's Enforcement Priorities in Applying Article 82 Ec Treaty to Abusive Exclusionary Conduct by Dominant Undertakings," *Official Journal of the European Union* (Dec. 3, 2008) // <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52009XC0224%2801%29> (asserting 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 *Konkurrensverket v. TeliaSonera Sverige AB*, No. C-52/09, 2011 E.C.R. I-527; Case *Deutsche Telekom AG v. Comm'n*, No. C-280/08 P, 2010 E.C.R. I-9555; Case *Telefónica and Telefónica de España v. Comm'n*, No. C-295/12, 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 Case *Pac. Bell Tel. Co. v. LinkLine Commc'ns, Inc.*, No. 555, 2009 U.S. 438.

⁶⁷ For an overview of exclusive dealing, see Case *Tomra Sys. ASA & Others v. Comm'n*, No. T-155/06, 2010 E.C.R. II-4361, and Case *Intel Corp. v. Comm'n*, No. C-413/14 P, 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

It seems unlikely that such an exclusive agreement would be imposed on a public blockchain, as this would imply the integration of such a condition from the beginning. In addition, once a transaction is registered on a blockchain, users have little interest in recording the transaction on another blockchain because such a move is costly. The technology itself therefore reduces the incentive to use several blockchains for the same transaction.

The situation is quite different for private blockchains. Foreclosing competitors is an effective way of increasing the blockchain's overall price for users and developers. In addition, private blockchains have an interest in increasing their attractiveness by obtaining data that they alone can provide. In the example of *BlockJobs*, Y may want to be the only company listing some types of job offers. To this end, *BlockJobs* may want to impose an exclusive dealing at the entry point of its blockchain. For this reason, it is highly likely that exclusive dealing practices will be implemented on private blockchains.

Rebates

Another related practice is to grant a customer retroactive rebates provided that he obtain all or most of its products or services from the dominant economic operator.⁶⁹ Since all practices are recorded and visible on public blockchains, one user's rebate will be visible to all and granting fidelity discounts could result in a rebuttal by users who do not benefit from such a rebate. This is more likely to occur if these benefits are perceived as unjustified by other users. Public blockchains therefore encourage 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 interest in attracting reputable users by offering discounts. Therefore, rebates are expected to appear on private block chains.

less than the roughly forty percent or fifty percent share usually required in order to establish a § 1 violation" (Case *United States v. Microsoft Corp.*, No. 253, 2001 F.3d 34).

⁶⁸ For an example, see Ethereum Foundation, Legal Agreement, [ethereum.org // https://www.ethereum.org/agreement](https://www.ethereum.org/agreement)

⁶⁹ For an overview of loyalty rebates, see Case *Intel Corp. v. Comm'n*, No. C-413/14 P, 2017 E.C.R. 632; Case *Hoffmann-La Roche and Co. AG v. Comm'n*, No. 85/76, 1979 E.C.R. 461; Case *Irish Sugar v. Comm'n*, No. T-228/97, 1999 E.C.R. II-2975; Case *British Airways v. Comm'n*, No. T-219/99, 2003 E.C.R. II-5925. In the United States, discount and rebate scheme programs can violate Section 2 of the Sherman Act. See Case *LePage's Inc. v. 3M*, No. 324, 2003 F.3d 141, 157; Case *Cascade Health Sols. v. PeaceHealth*, No. 502, 2007 F.3d 895, 905; Case *Eisai Inc. v. Sanofi-Aventis U.S.*, No. 08-4168, 2014 WL 1343254, at *12.

2.2.2. EXPLOITATIVE ABUSES

This section aims to describe how exploitative abuses could be implemented on blockchain. Exploitative abuse consists in imposing directly or indirectly unfair conditions on existing customers or suppliers.⁷⁰ Under such a policy, abusive exploitation can occur when blockchain creators provide services in exchange for preferential treatment⁷¹ or when one blockchain imposes adverse measures on another blockchain or when one blockchain imposes unfavorable measures on another blockchain. In the *BlockJobs* example, Y can impose unfair conditions that users are not willing to pay for to gain visibility on *BlockJobs*. However, since blockchain is still evolving rapidly, there is little use in focusing too much on exploitative abuse. The dynamism of the blockchain environment will likely correct these abuses themselves. This type of abuse is nonetheless possible and will undoubtedly be the subject to legal proceedings.

2.2.3. DISCRIMINATORY ABUSES

Discriminatory abuses occur when parties apply “dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage”.⁷² There are several of these types of abuse, price discrimination being the most common.⁷³ 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.”⁷⁴

⁷⁰ 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 (European Union, *Consolidated Version of the Treaty on the Functioning of the European Union*, Official Journal (2012) // <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT> [hereinafter TFEU]). See Case *Hynix Semiconductor Inc v. Infineon*, No. COMP/38.636, 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.

⁷¹ Østbye, *supra* note 63.

⁷² Robert O'Donoghue and Jorge Padilla, *The Law and Economics of Article 102 TFEU* (Oxford: Hart Publishing, 2013), 43.

⁷³ In European judicial history, there are few cases in which price discrimination alone was found abusive. See Case *Clearstream Banking AG v. Comm'n*, No. T-301/04, 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 Case *Post Danmark A/S v. Konkurrencerådet*, No. C209/10, 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 Case *Blue Cross & Blue Shield United of Wis. v. Marshfield Clinic*, No. 65, 1995 F.3d 1406, 1413. Price discrimination may also violate the Robinson-Patman Act. See Case *Brooke Group Ltd. v. Brown & Williamson Tobacco Corp.*, No. 509, 1993 U.S. 209, 220.

⁷⁴ Richard Posner, *Antitrust Law* (Chicago: University of Chicago Press, 2001), 35.

Since price discrimination involves favoring certain customers over others, it usually occurs in two ways: by charging different prices to different customers for the same product, or charging some customers the same price for different products.

Because of the “visible effect” of public blockchains, cases of price discrimination will be limited. However, within private blockchains users may encounter discriminatory terms, as applying different terms to different users is an effective way to encourage users to join and use the blockchains. Discriminatory pricing may encourage some users to remain active in the blockchain by offering lower prices, thus creating a potential claim for discrimination. As a result, discriminatory abuses are more likely to occur 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 antitrust authorities’ concerns.

CONCLUSION

The decentralized nature of the blockchain itself is designed to prevent the creation of monopolies. Its idea is that all market participants retain the ability to make decisions without having to follow the instructions of a centralized economic force. It is not blockchain in itself but a pricing policy that can serve as an abuse of a dominant position. Therefore, the concerns of interested parties that their unique blockchain is being abused at this stage of the evolution of the blockchain can be considered unjustified. At the current stage corporations should not refuse serious consideration of the possibilities of blockchain technology for reasons of competition.

This article has identified several anti-competitive practices. One of the main conclusions of this study is that most of the usual antitrust instruments will be ineffective against public blockchain⁷⁵ since antitrust law do not provide complete answers to three questions: how are anti-competitive practices committed on public “permission-less”⁷⁶ to be detected, how is the economic operator responsible for these practices to be identified, and, lastly, how are they to be remedied in the future? While the author of an anti-competitive practice on blockchain can sometimes be identified, the effectiveness of sanctions and remedies may be hindered by the immutability⁷⁷ of the blockchain.⁷⁸

⁷⁵ Timothy May, “The Crypto Anarchist Manifesto,” *Activism* (1992) // <https://www.activism.net/cypherpunk/crypto-anarchy.html>.

⁷⁶ Public blockchains are also called “permission-less” or “open” blockchains.

⁷⁷ Presciently, the home page of the Ethereum Project reads: “Build unstoppable applications.” See “Ethereum” // <https://www.ethereum.org/>

The situation is different for private permissioned blockchains. The most obvious of the real antitrust risks may be associated with restricting access to the private blockchain and the exchange of competitively sensitive data within the blockchain consortium. On this type of blockchain, antitrust issues such as refusal to deal, margin squeezing or predatory pricing most often occur in the context 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, and they should point to procompetitive justifications.

Another challenge to competition with regard to the use of blockchain within the legislation of the EU in the field of legislative regulation of the blockchain in the frame of competitive policies, lies in the enforcement by centralized regulators such as the DoJ, the FTC or the European Commission, of vertically designed rules and concepts of antitrust law to a technology built around the desire for decentralization.⁷⁹ There is the need to find new ways of decentralizing antitrust law and antitrust authorities⁸⁰ through the design⁸¹ and the implementation of new governance models using blockchain.⁸²

On the whole, international legislation generally and EU legislation in particular must adapt to new legal relationships that appear, generated by new technologies, to include provisions aimed at protecting the rights of consumers of such technologies, norms on money laundering, market manipulation, insider information, etc. Due to the inherent cross-border nature of the blockchain, it is also necessary to harmonize legislation among states, in particular with regard to the establishment of applicable law. Thus, we can confidently predict significant changes that the blockchain is able to bring to almost all sectors of the economy.

Future research in the field of competition policy with regard to blockchain may be related to the development of special legal regimes (regulatory sandboxes),

⁷⁸ Guegan, *supra* note 26, 17020.

⁷⁹ Kevin Werbach, *The Blockchain and the New Architecture of Trust* (Cambridge: MIT Press, 2018), 16.

⁸⁰ Maurice. Freedman, *Capitalism and freedom* (Chicago: University of Chicago Press, 1962), 33.

⁸¹ On how to design competition agencies, see Frederic Jenny, "The Institutional Design of Competition Authorities: Debates and Trends"; in: *Competition law enforcement in the BRICS and in developing countries* (2016) // https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894893. See also OECD, "Roundtable on Changes in Institutional Design," DAF/COMP/M(2015)1/ANN6/FINAL // [https://one.oecd.org/document/DAF/COMP/WP2/M\(2015\)1/ANN6/FINAL/en/pdf](https://one.oecd.org/document/DAF/COMP/WP2/M(2015)1/ANN6/FINAL/en/pdf); Michael Abramowicz, "Cryptocurrency-Based Law," *Arizona Law Review* 58 (2016): 359 ("Peer-to-peer law is likely to emerge slowly and in unpredictable ways, but it has the potential to create authoritative decisions without authoritative decision-makers. There may be decisive arguments against particular peer-to-peer institutions, but legal theorists should at least allow peer-to-peer institutions to join the menu of possible regulatory arrangements."). Decentralized antitrust authorities could use futarchy, quadratic voting, and liquid democracy or holacracy mechanisms.

⁸² *Ibid.*: 359.

where blockchain developers can test the technology to solve existing problems of competition regulation.

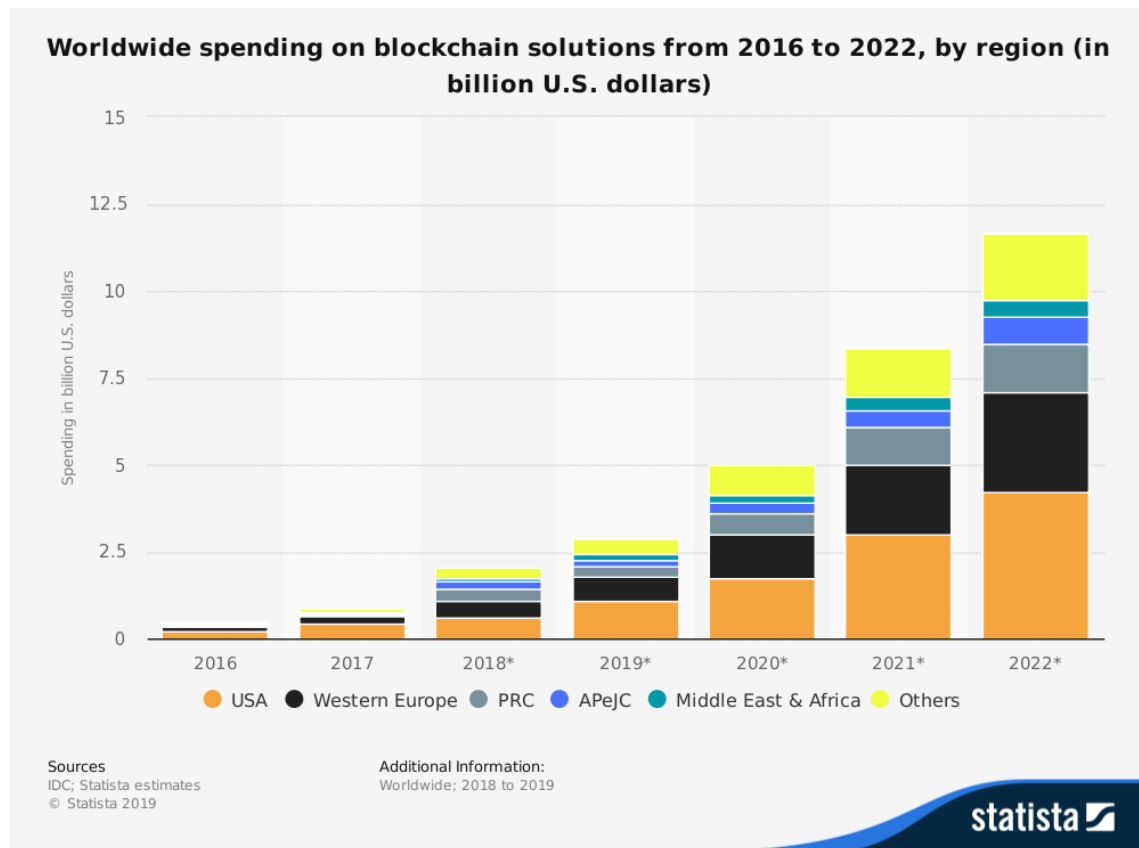


Fig. 1. Worldwide spending on blockchain solutions from 2016 to 2022, by region (in billion U.S. dollars)⁸³

BIBLIOGRAPHY

1. Abramowicz, Michael. "Cryptocurrency-Based Law." *Arizona Law Review* 58 (2016): 359-420.
2. Bradley, Robert. "On the Origins of the Sherman Antitrust Act." *Cato Journal* 9 (1990): 737-742.
3. Champagne, Phil. *The book of Satoshi: The collected writings of Bitcoin creator Satoshi Nakamoto*. USA: e53 Publishing, 2014.
4. Comm'n of The European Communities, "Guidance on the Commission's Enforcement Priorities in Applying Article 82 Ec Treaty to Abusive Exclusionary

⁸³ Information taken from: <https://www.martechvibe.com/insights/staff-articles/everything-you-need-to-know-about-blockchain-in-marketing/>.

- Conduct by Dominant Undertakings," *Official Journal of the European Union* (Dec. 3, 2008) // <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52009XC0224%2801%29>.
5. Cong, Lin, and Zhiguo He. "Blockchain Disruption and Smart Contracts." *The Review of Financial Studies* 32 (2018): 1754-1797.
 6. Cuccuru, Pierluigi. "Beyond Bitcoin: An Early Overview on Smart Contracts." *International Journal of Law and Information Technology* 25 (2017): 179-195.
 7. Dannen, Chris. *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*. New York: Apress, 2017.
 8. De Filippi, Primavera. *Blockchain and the law: the Rule of Code*. Boston: Harvard University Press. 2018.
 9. Desal, Kiran. *Blockchain and competition law*. London: Ernest & Young Law Alert, 2018 // [https://www.ey.com/Publication/vwLUAssets/ey-blockchain-and-competition-law/\\$FILE/ey-blockchain-and-competition-law.pdf](https://www.ey.com/Publication/vwLUAssets/ey-blockchain-and-competition-law/$FILE/ey-blockchain-and-competition-law.pdf).
 10. Economides, Nicholas, and Ioannis Lianos. "Elusive Antitrust Standard on Bundling in Europe and in the United States in the Aftermath of the Microsoft Cases." *Antitrust law Journal* 76 (2010): 483-494.
 11. European Central Bank. "Why does the ECB have a stake in market infrastructure?" (2016) // <https://www.ecb.europa.eu/pub/annual/special-features/2016/html/index.en.html>.
 12. Freedman, Maurice. *Capitalism and freedom*. Chicago: University of Chicago Press, 1962.
 13. Guegan, Dominique. "Public Blockchain Versus Private Blockchain." *Documents de travail du Centre d'Economie de la Sorbonne* 1 (2017): 17020 // <https://halshs.archives-ouvertes.fr/halshs-01524440/document>.
 14. Hong, Sunghyuck. "P2P networking based internet of things (IoT) sensor node authentication by Blockchain." *Peer-to-Peer Netw.* 13 (2020): 579-589.
 15. Hovenkamp, Herbert J. "The Rule of Reason." *Florida Law Review* 70 (2018): 81-96.
 16. Huberman, Gur, Jacob Leshno, and Ciamac Moallemi. "An Economic Analysis of the Bitcoin Payment System." *Columbia Business School Research Paper* 2 (2017): 17-92.
 17. IDC Trackers. "Worldwide Blockchain Spending Guide" // https://www.idc.com/tracker/showproductinfo.jsp?prod_id=1842.

18. Jenny, Frederic. "The Institutional Design of Competition Authorities: Debates and Trends," In *Competition law enforcement in the BRICS and in developing countries*, pp. 1-57 (2016) // https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894893.
19. Kim, Seoung. "Ethereum Upgrades as Hard Forks Activate on Blockchain." *Coindesk*, (2019).
20. Lianos, Ioannis. "Blockchain Competition." *CLES Research Paper Series* 4/2018 (2018) // https://sci-hub.tw/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3257307.
21. Mauri, Ross. "Three Features of Blockchain that Help Prevent Fraud." *IBM* (2017) // <https://www.ibm.com/blogs/blockchain/2017/09/three-features-of-blockchain-that-help-prevent-fraud>.
22. May, Timothy. "The Crypto Anarchist Manifesto." *Activism* (1992) // <https://www.activism.net/cypherpunk/crypto-anarchy.html>.
23. Miseviciute, Jurgita. "Blockchain and virtual currency regulation in the EU." *Journal of Investment Compliance* 19 (2018): 33-38.
24. Nakamoto, Satoshi. "Bitcoin: a peer-to-peer electronic cash system." *Bitcoin* (2008) // <https://bitcoin.org/bitcoin.pdf>.
25. O'Donoghue, Robert, and Jorge Padilla. *The Law and Economics of Article 102 TFEU*. Oxford: Hart Publishing, 2013.
26. OECD. *Blockchain Technology and Competition Policy: Issues Paper by the Secretariat*. OECD, 2018 // [https://one.oecd.org/document/DAF/COMP/WD\(2018\)47/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf).
27. OECD. "Roundtable on Changes in Institutional Design." DAF/COMP/M(2015)1/ANN6/FINAL // [https://one.oecd.org/document/DAF/COMP/WP2/M\(2015\)1/ANN6/FINAL/en/pdf](https://one.oecd.org/document/DAF/COMP/WP2/M(2015)1/ANN6/FINAL/en/pdf).
28. Østbye, Peder. "The Adequacy of Competition Policy for Cryptocurrency Markets." *Social Science Research Network* (2017) // <https://www.competitionpolicyinternational.com/the-adequacy-of-competition-policy-for-cryptocurrency-markets/>.
29. Østbye, Peder. "The Case for a 21 Million Bitcoin Conspiracy." *Journal of Financial Transformation* 48 (2018): 88-97.
30. Penz-Sharp, Alan. "Blockchain for Business: Ready or Not, Here it Comes." *CMSWire* (2017) //

<https://www.cmswire.com/information-management/blockchain-for-business-ready-or-not-here-it-comes>.

31. Posner, Eric, and Glen Weyl. *Radical Markets: uprooting capitalism and democracy for a just society*. Princeton: Princeton University Press, 2018.
32. Posner, Richard. *Antitrust Law*. Chicago: University of Chicago Press, 2001.
33. Raval, Siraj. *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*. Sebastopol: O'Reilly Media, 2016.
34. Roberts, Russ, and Jim Epstein. "Jim Epstein on Bitcoin, the Blockchain, and Freedom in Latin America." *Econ Talk* (2017) // <http://www.econtalk.org/jim-epstein-on-bitcoin-the-blockchain-and-freedom-in-latin-america/>.
35. Rochet, Jean-Charles, and Jean Tirole. "Platform Competition in Two-Sided Markets." *Journal of the European Economic Association* 1 (2003): 990-1029.
36. Swan, Melanie. *Blockchain: Blueprint for a new economy*. Sebastopol: O'Reilly Media, 2015.
37. Talamo, Maurizio, Franco Arcieri, Andrea Dimitri, and Christian H. Schunck, "A Blockchain based PKI Validation System based on Rare Events Management." *Future Internet* 12 (2020): 40.
38. Tapscott, Don, and Alex Tapscott. *A Blockchain Revolution: how the technology behind Bitcoin is changing money, business and the world*. New York: Penguin Random House, 2016.
39. The World Bank. "Blockchain or distributed ledger technology." *The World Bank Group* (2018) // <http://documents1.worldbank.org/curated/pt/260121548673898731/pdf/134063-WP-121278-2nd-edition-IFC-EMCompass-Blockchain-Report-PUBLIC.pdf>.
40. Thomas, Ryan "Blockchains and Antitrust: new technology, same old risks." *JonesDay One Firm Worldwide Whitepaper* (2018) // <https://www.jonesday.com/blockchains-and-antitrust-new-technology-same-old-risks-08-02-2018/>.
41. Tsu, Sun. *The Art of War*. London: Macmillan, 2017.
42. Vigna, Paul, and Michael Casey. *The Truth Machine: the Blockchain and the Future of Everything*. New York: St. Martin's Press, 2018.
43. Walch, Angela. "The Path of the Blockchain Lexicon (and the Law)." *Review of Banking & Financial Law* 36 (2017): 713-718.
44. Werbach, Kevin. *The Blockchain and the New Architecture of Trust*. Cambridge: MIT Press, 2018.
45. Werbach, Kevin. "Trust, but Verify: Why the Blockchain Needs the Law." *Berkeley Technology Law Journal* 33 (2018): 487-495.

46. World Economic Forum. "Deep Shift: Technology Tipping Points and Societal Impact" (2015) // <https://www.weforum.org/reports/deep-shift-technology-tipping-points-and-societal-impact>.
47. Zamfir, Vlad. "Introducing Casper 'The Friendly Ghost'." *Ethereum Blog* (2015) // <https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost>.

LEGAL REFERENCES

1. *Blue Cross & Blue Shield United of Wis. v. Marshfield Clinic*. (1995) 65, F.3d 1406, 1413.
2. *British Airways v. Comm'n*. (2003) T-219/99, E.C.R. II-5925.
3. *Brooke Group Ltd. v. Brown & Williamson Tobacco Corp.* (1993) 509, U.S. 209, 220.
4. *Cascade Health Sols. v. PeaceHealth*. (2007) 502, F.3d 895, 905
5. *Clearstream Banking AG v. Comm'n*. (2009). T-301/04, E.C.R. 317.
6. *Consolidated Version of the Treaty on the Functioning of the European Union*. Official Journal (2012) // <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT> [hereinafter TFEU]).
7. *Deutsche Telekom AG v. Comm'n*. (2010) C280/08 P, E.C.R. I-9555.
8. *Eisai Inc. v. Sanofi-Aventis U.S.* (2014) 08-4168, WL 1343254, at *12.
9. *European Night Servs. Ltd. (ENS) v. Commission*. (1998) T-374/94, T375/94, T-384/94, and T-388/94, E.C.R. II-3141;
10. *Google Shopping*. (2017) 39740, E.C.R. 145.
11. *Hynix Semiconductor Inc v. Infineon*. (2010) COMP/38.636, O.J. C 30.
12. *Hoffmann-La Roche and Co. AG v. Comm'n*. (1979) 85/76, E.C.R. 461
13. *Illinois Tool Works Inc. v. Independent Ink, Inc.* (2006) 547, U.S. 28.
14. *Intel Corp. v. Comm'n*. (2017) C-413/14 P, E.C.R. 632
15. *Irish Sugar v. Comm'n*. (1999) T-228/97, E.C.R. II-2975
16. *Jefferson Parish Hosp. District No. 2 v. Hyde*. (1984) 466, U.S. 2, 1
17. *Konkurrensverket v. TeliaSonera Sverige AB*. (2011) C-52/09, E.C.R. I-527.
18. *LePage's Inc. v. 3M*. (2003) 324, F.3d 141, 157
19. *Microsoft Corp. v. Sun Microsystems, Inc, Comm'n Decision*. (2004) 3/37.792.
20. *Oscar Bronner v. Mediaprint Zeitungs und Zeitschriftenverlag*. (1998) C-7/97, E.C.R. I-7796.
21. *Pac. Bell Tel. Co. v. LinkLine Commc'ns, Inc.* (2009) 555, U.S. 438.

22. *Post Danmark A/S v. Konkurrencerådet*. (2012) C209/10, E.C.R. 172.
23. *Telefónica and Telefónica de España v. Comm'n.* (2013) C-295/12, E.C.R. 619.
24. *Tomra Sys. ASA & Others v. Comm'n.* (2010) T-155/06, 2010 E.C.R. II-4361
25. *United States v. Microsoft Corp.* (2001) 253, F.3d 34.
26. *Verizon Comm. Inc. v. Law Offices of Curtis V. Trinko, LLP.* (2004) 540, U.S. 398