HELLENIC REPUBLIC
National and Kapodistrian
University of Athens
EST. 1837

LAW SCHOOL

LL.M in International & European Legal Studies

LL.M. Course: Private Law & Business Transactions

Academic Year: 2020-2021

DISSERTATION

of Evangelia Spyropoulou

Student's Registration Number: 734002 0120024

Blockchain Technology and Competition Policy within the European Legislative Framework

<u>Examination Board:</u>

Alexandra Mikroulea, Associate Professor (Supervisor)

Antonios Karampatzos, Professor

George Dellis, Professor

Athens, 14.11.2021

‘’The intersection of law, politics, and technology is going
to force a lot of good thinking.’’
-Bill Gates

The opinions and positions argued in this paper only express the author and should not be considered as representing the official positions of the National and Kapodistrian University of Athens.

ABSTRACT

Law and Technology have historically been foundational interconnected aspects of a well-functioning, equitable and prospering society. The proliferation of disrupting technological applications over the last years, however, has posed new questions in regards to how can Law adapt to a rapidly changing technological and economic environment. The blockchain technology is one of the most recent disrupting technological innovations with high potential to disrupt the established transaction, transfer, and registration systems, and the way markets and institutions function across the world. This creates significant new challenges for governments and competition authorities in ensuring free and fair competition and regulatory certainty.

This thesis aims to present how the blockchain technology interacts with Competition Law and Policy within the European Legislative Framework. Research focuses on the characteristics and uses of Blockchain Technology, such as its decentralized and distributed character. The existing Competition Legislative Framework is reviewed, focusing on the Art. 101 and Art. 102 of Treaty of Functioning of European Union (TFEU), along with notable cases and their verdicts, highlighting the potential issues and violations that may occur from the interaction between blockchain technology and Competition Law.

The issues arising from the application of legal rules, creation of legislative policies and the general fitting of the blockchain technology in the existing Competition Legislative Framework are discussed. The analysis reveals that competition authorities are facing major challenges in accounting for the Blockchain Technology's innovations, in particular on anticompetitive agreements and abuse of dominant position. The innovative technical characteristics of blockchain technology as well as its way of functioning are not in line with the foundational aspects and the logic on which Competition Law is built. This results in serious problems when it comes to applying competition rules in blockchain platforms, as blockchain technology can be used to facilitate anti-competitive practices and gain unfair competitive advantages.

However, the analysis also underscores that the blockchain technology can and should be used as a novel tool by competition authorities to better enforce competition law. This can be achieved through the use of smart contracts to ensure compliance with competition requirements and commitments, and verifiable information stored on blockchain ledgers to provide evidence on anti-competitive conduct and collusion cases, as well as streamline leniency programs. Overall, utilizing blockchain applications would not only make the competition law enforcement process more effective and transparent, but also result in considerable cost savings by minimizing the time and effort required to monitoring compliance and implementation.

Governments and competition authorities should focus on better understanding the design protocols of blockchains and aim to actively participate in the development of new blockchains. However, it is important to properly evaluate the key risks in utilizing blockchain applications more broadly. Market studies would help competition authorities properly evaluate the potential barriers, threats, and opportunities in integrating blockchain technology into Competition Law, and update their governance models to encompass the decentralized and distributed characteristics of the blockchain.

Table of Contents

1. INTRODUCTION

1.1 Context

On the onset of their creation, Law and Technology were meant to aim at a smooth and orderly functioning of the society in which they were developed. Nevertheless, this is not the only common aim and characteristic of Law and Technology. Both of them are presented through a complex structure, with a lot of reasoning and analysis behind and moreover, both of them are concepts that cannot be static. They adjust each time to the new society data, to the political and economic trends, to the new human needs. Law and Technology are both progressive concepts.

It is undoubtable that we live in an era of astounding technological transformation. Information Technology has marked the start of a wholly new way of thinking, interacting, and trading in modern societies. It could be characterized as a revolution so profound, as the two great technological revolutions of the past—the agricultural and industrial revolutions. In this technological transformation where change, not stability has become the norm, someone could raise the question how legal stability and predictability, as ancillary characteristics of the configuration of legislation and legal policies, can adjust with the best possible way.

This is a question that concerns both scientific worlds -the legal and the technological one upon which lot of opinions have been expressed and there is space for a lot more to be. The crucial point and common characteristic of all of the until now formulated ideas regarding the co-existence and cooperation of Law and Technology could be summarized in the worlds of Lawrence Lessig ‘’Law and technology can produce, together, a kind of regulation of creativity we've not seen before’’.

The Blockchain Technology is a prime example of a novel technological innovation with the potential to substantially and rapidly disrupt how people live and work. Like many disrupting technological innovations, however, it has also created a new set of challenges for legislative frameworks, and competition law and policy in particular.

Governments and regulators are still trying to assess how the Blockchain Technology works and its impacts for policy-making, especially whether and how should competition law and policies be updated to account for its innovative aspects. Many laws and regulatory frameworks were developed several years or even decades ago, when aspects such as decentralized and distributed data exchange and smart, permissionless contracts were just theoretical concepts.

As such, it is crucial to better understand the Blockchain Technology’s implications for competition law and policy in order to jump-start regulatory updates and address the gaps in the existing legislative frameworks. This would help provide governments and regulators with powerful new tools to maintain free and fair competition, ensure regulatory certainty, and minimize business risks.

1.2 Research Aims

The purpose of this dissertation is to evaluate how a specific field of Information Technology, the so called Blockchain Technology, interacts with Competition Law and Policy within the European Legislative Framework. In order to do so, the dissertation reviews how the Blockchain Technology works, its uses and categories, and the issues arising when it comes to application of legal rules, creation of legislative policies and the fitting of the Blockchain Technology in the existing Competition Legislative Framework – and vice versa.

1.3 Methodology

The dissertation is divided in two main parts. The first part presents the Blockchain Technology and the structure of a blockchain network, as well as its categories, including open/public, closed/ private, and permissionless/permissioned blockchain networks, laying the foundation for the analysis in the second part of the dissertation. An overview of the characteristics of Blockchain Technology is provided, focusing on the Distributed Ledger Technology (DLT) to highlight the decentralized and distributed attributes of a blockchain. The two major consensus mechanisms used to verify and specify legitimate transactions through blockchains, Proof of Work (PoW) and Proof of Stake (PoS), are then described.

The second part of the dissertation reviews the co-existence of Blockchain Technology and European Competition Policy. The existing Competition Legislative Framework is examined, with particular emphasis on the Art. 101 and Art. 102 of Treaty of Functioning of European Union (TFEU). In order to highlight the issues arising from the interaction between Blockchain Technology and competition law, each possible violation that may occur following the order that these are presented in the aforementioned articles is assessed.

Starting with a reference to general questions and potential problems that have been posed by legal and economic experts across the so far written literature, including papers, books and articles, the major challenges that competition authorities are facing are defined. Then, the analysis focuses on two primary aspects of competition law: anticompetitive agreements and abuse of dominant position. After referring to some notable cases such as the Libra case, United American Corp v Bitmain Inc, Gallagher Vs Bitcointalk.org , research continues with a review of all the topics mentioned so far and a commentary of what is written, set and said regarding our topic.

The last part of the dissertation presents the conclusions that could be made as to the potential arising challenges and the possible solutions to address them. Last but not least, a unique section will discuss the possibility of Blockchain Technology to be used as a tool in the hands of the Competition Committee to better enforce competition law as well as improve the effectiveness and transparency of the enforcement process, and the possible ways that this can happen.

2. MAIN PART – PART A

2.1 Blockchain Technology as an Innovative Intervention in the Capital Markets System

Over the last years, the blockchain technology has become increasingly attractive to companies and governments as it could provide novel solutions to the well-cited issue of mutability in transactions.[1] It appears as a general-purpose technology that threatens to disrupt markets and institutions across the world[2], and as a highly innovative means able to change the so far established transaction, transfer and registration system. Even though it could be a fundamental new solution for governments and the average person, many regulatory agencies and people do not know exactly how this technology functions. Therefore, the primary and first question requiring an answer is: what is -in simple words- Blockchain Technology and how does it work?[3]

Blockchain is a system for recording information, with the particular characteristic that this recording happens in a way that diminishes the likelihood of hacking and/or tricking the system. It sums up the following technologies:

1. The private key cryptography
2. The Distributed Ledger Technology (DLT)[4]
3. The verification of transactions and data, through the use of large computing power on the part of register participants by providing an incentive in return for disturbing network service.[5]

More specifically, blockchain is a digital ledger of data and information, including transactions, in which the data are encrypted with a procedure named hashing.[6] Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. As such, these data are needed to be verified by participants in the network through an algorithmic confirmation process in order to be part of this group of entries (block). It is important to mention that each blockchain functions based on its own whitepaper, whose terms people are asked to agree on before they become part of the network.

[1] M. Artzt and Richter, T. 2020. Handbook of Blockchain Law: A Guide to Understanding and Resolving the Legal Challenges of Blockchain Technology. Kluwer Law International BV 2020, page 2

[2] Pike, C, and A. Capobianco (2020), Antitrust and the trust machine, http://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf, page 5

[3] Lianos, I. 2018. Blockchain and Competition. London: Centre for Law, Economics and Society (CLES), page 3-5

[4] Distributed Ledger Technology (DLT) refers to the technological infrastructure and protocols that allows simultaneous access, validation, and record updating in an immutable manner across a network that's spread across multiple entities or locations.

[5] O.S Androtsopoulou Olga, Blockchain Technology: Risks and Opportunities, 2019, pages 14-16

[6] Hashing is a method of cryptography that converts any form of data into a unique string of text. Any piece of data can be hashed, no matter its size or type. In traditional hashing, regardless of the data's size, type, or length, the hash that any data produces is always the same length.

2.2 Characteristics of a Blockchain Network

A blockchain network has certain characteristics that are unique among the so far known ledgers. More specifically, the blockchain ledger is programmable, secure, and could be unanimous or anonymous. It is immutable, contains timestamps, and its most important and innovative characteristic is that it is distributed and decentralized.

Figure 1 shows a brief explanation of the special characteristics of Distributed Ledger Technology. The following sections focus on analyzing further the importance of Decentralization and Distribution.

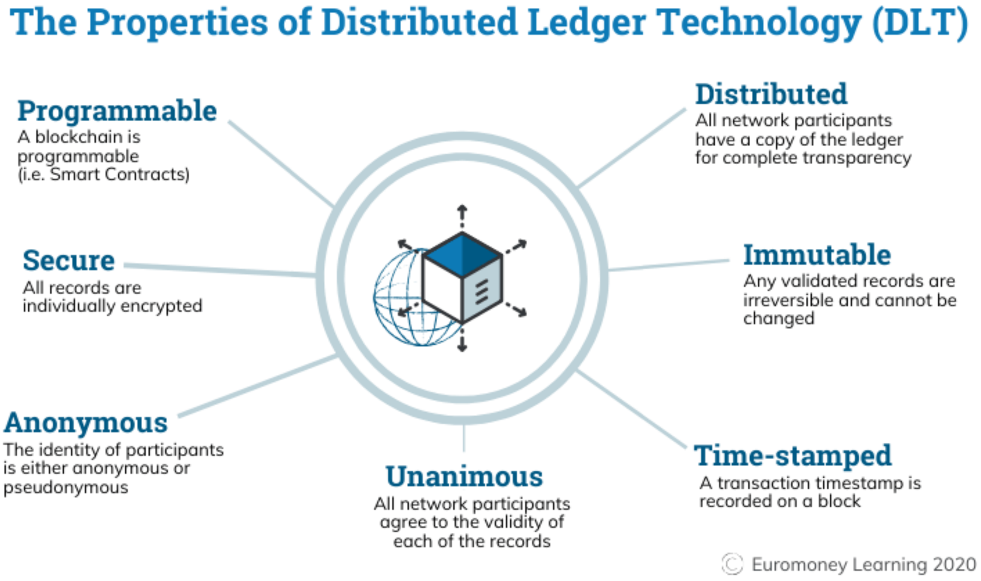

The Properties of Distributed Ledger Technology (DLT)
Programmable
A blockchain is programmable (i.e. Smart Contracts)
Distributed
All network participants have a copy of the ledger for complete transparency
Secure
All records are individually encrypted
Immutable
Any validated records are irreversible and cannot be changed
Anonymous
The identity of participants is either anonymous or pseudonymous
Unanimous
All network participants agree to the validity of each of the records
Time-stamped
A transaction timestamp is recorded on a block
© Euromoney Learning 2020

Figure 1. Properties of Distributed Ledger Technology.[7]

2.2.1 Decentralization – Bitcoin as a decentralized blockchain technology

In regards to blockchain, decentralization refers to the transfer of control from a centralized entity or group, to a distributed network. This characteristic of blockchain technology can be crucial when it comes to controlling potential anti-competitive behaviors – and in the following sections we will analyze briefly how exactly this creates the so-called Antitrust paradox and has been an issue that has concerned man y legal experts, especially when it comes to issues relevant with anti-monopolistic legislation.

To make the concept of decentralization more understandable, it could be useful to see it as an example based on one of the most known uses of Blockchain Technology, cryptocurrencies,

[7] Euromoney Institutional Investor PLC. (2020). Euromoney Expertise: What is Blockchain., page 2

and more specifically Bitcoin.[8] Bitcoin, as a data base needs a collection of computers to store its blockchain which functions as a specific type of database that stores every Bitcoin transaction ever made.[9] Unlike the so far existing databases of this kind, where all computers are controlled by a ‘’center’’, in Bitcoin every computer or group computers are controlled by individuals or groups of individuals.

Let’s use the example of an entity that has a large proprietary server database with hundreds of personal computers containing project and client data. The difference with Bitcoin is that Bitcoin’s database also utilizes hundreds of personal computers, but instead of being kept under a single entity’s server, these computers are distributed across the world and operated by many different people. [10] As such, the Bitcoin platform operates in a decentralized manner. This does not mean that centralized blockchains can not or do not exist.

The question is why decentralization matters. It is worth mentioning that decentralization is not a new concept. A new technological innovation might be centralized, distributed, and/or decentralized. While blockchain applications are often based on decentralized networks, they are not always categorized as decentralized.

The concept of decentralization, thus, should be applied across all aspects of a new blockchain application, from its initial development and all the way to the management of information by the users. Decentralized applications might also result in less efficient transaction processes, but they do provide a more fair and equitable management system.[11]

In the main part of this project, we will analyze briefly how this characteristic of blockchain networks raises a lot of important issues, due to the fact that all the anti-monopolistic legislation is based in the idea of an entity, an undertaking that has a center of control, through which the competition authorities can actually perform any investigation or press any charges. [12]

2.2.2 Distribution

Another notable and unique characteristic of blockchain data bases is distribution. But what is actually meant by a blockchain network being distributed? A distributed ledger is a database that is consensually shared across multiple sites around the world and is accessible by multiple people. This practically means that each transaction has ‘’witnesses’’, since anyone can have – and has- access in the data of this transaction. [13]

The immediate consequences of this are of great interest. Firstly, a distributed network removes the need for a central authority to provide safety and security against mismanagement

[8] Digital currency which operates free of any central control or the oversight of banks or governments.
[9] Op. Cit. note 5 page 21

[10] Albertorio, A. "Simply Explained: Why is Proof of Work Required in Bitcoin?" January 7, 2020. Accessible in https://medium.com/coinmonks/simply-explained-why-is-proof-of-work-required-in-bitcoin-611b143fc3e0

[11] Conway, L. 2021. "Blockchain Explained." Investopedia. June 1. https://www.investopedia.com/terms/b/blockchain.asp#decentralization.
[12] See below in the main part for more details
[13] Op. Cit note 5 pages 16-20

and fraud. In this manner, a central authority is not needed to authorize or validate any transactions, as it used to be necessary until very recently in transaction history. Within the spectrum of the current competitive legislative framework, as it is more detailed explained in the main part of this project, the aforementioned need of a central authority highlights an interesting point from a legal and economic point of view, since this ''check'' against mismanagement and fraud was up to now the role that competition authorities used to play.

Secondly, this system can provide a lot of more security and trust built between the parties of the transaction, as all the information on the ledger is securely and accurately stored using cryptography and can be accessed using keys and cryptographic signatures. Once the information is stored, it becomes an immutable database, which the rules of the network govern.

In other words, the distribution allows the abolishment of the middleman. This abolishment is of a great interest from an economic as well as from a legal point of view. The traditional model of distribution tended to favor distributors and for a lot of people the absence or the decrease of their role is positive evolution. This new model would allow the control of the network and its profits to move towards content creators. In this way, the blockchain technology can significantly disrupt the business-as-usual methods of producing goods and services.[14]

In conclusion, distribution allows the absence of the middleman, making the Blockchain Technology different from the so far existing data bases in a digital form and allows them to develop a self-auto-controlled system.

2.3 Blockchain Network Consensus Mechanisms: Proof of Work and Proof of Stake

Proof of work (PoW) and proof of stake (PoS) are the two major consensus mechanisms cryptocurrencies use to verify new transactions, add them to the blockchain, and create new tokens. Consensus mechanisms is the system used by the computers in a crypto network allowing them to indicate which transactions are legitimate.[15]

More specifically, PoW is the original consensus algorithm in a blockchain network, an idea closely related to mining.[16] Virtual miners around the world are part of a race to be the first to solve a math puzzle. The incentive for this is the reward that the network offers to the miner that solves the riddle and gets to update the blockchain with the latest verified transactions. This reward is given in a predetermined number of cryptocurrencies within this network. The reason it is called "proof of work" is because the network requires an enormous amount of processing power.[17]

The arising question is why PoW is needed. The answer is highly connected with the fact that blockchain networks are decentralized and peer-to-peer by design.[18] PoW is necessary for

[14] Op. Cit note 10

[15] Op. Cit page 37

[16] Mining is the process of gaining cryptocurrencies by solving cryptographic equations with the use of high-power computers

[17] Kumar, K. 2021. Proof Of Work In Blockchain | What Is Proof Of Work | Proof Of Work Explained | Simplilearn. Directed by Krishna Kumar.

[18] Note 16 page 38

security, which prevents fraud and enables trust. The security ensures that independent data processors (miners) can not lie about a transaction. [19]

Proof of Stake (PoS) comes as an alternative to PoW, since the last one appears to encourage the use of mining pools[20]. The upcoming danger in this use is that it makes blockchains more centralized as opposed to decentralized.[21]Furthermore, while PoW requires massive amounts of energy, with miners needing to continuously sell their coins, PoS gives mining power based on the percentage of coins held by a miner.

This practically means that the more coins a miner owns, the more mining power he has. Therefore, there is an election process in which one node is selected to validate the block. The validator[22] has to deposit a certain amount of coins in the network as stake, in order to be eligible for the process. The size of the stake determines his chances to be chosen to force the next block.

Proof of stake has some notable advantages. It is also claimed to be less risky in terms of the potential for miners to attack the network, as it structures compensation in a way that makes an attack less advantageous for the miner.[23] Last but not least, there are some cases where Proof of Work and Proof of Stake can co-exist in the system. This can happen when the structure of some cryptocurrencies dictates the generation of new blocks by miners and, subsequently, the confirmation of these by ‘’master’’ nodes selected under the PoS procedure.

2.4 Blockchain Categories

2.4.1 Open/Public and Closed/Private Blockchain Networks

- **Open-Public Blockchain Network**

A public blockchain network is a blockchain network where anyone can join whenever they want. There are no restrictions when it comes to participation. More so, anyone can see the ledger and take part in the consensus process.

A public blockchain network is also verified by more independent participants, called nodes.[24] This characteristic is highly important when it comes to enabling almost anyone to access the data of the blockchain platform and it empowers the aforementioned decentralized character of the blockchain network.

A public blockchain Network can be permissioned, where certain rules are applied in order to identify the participants in a transaction within the network (this mainly concerns retail sales)

[19] Op. Cit. note 10 pages 33-37

[20] Mining pool is the joint group of cryptocurrency miners who combine their computational resources over a network to strengthen the probability of finding a block or otherwise successfully mining for cryptocurrency

[21] Jakobsson, M., and Juels, A. 1999. Proofs of Work and Bread Pudding Protocols.
Deventer: Kluwer, B.V. , page 3

[22] Validator is used in Proof of Stake instead of Minor

[23] Huilet, M. 2020. Bitcoin Will Follow Ethereum And Move to Proof-of-Stake. April 4, accessible in https://cointelegraph.com/news/bitcoin-will-follow-ethereum-and-move-to-proof-of-stake-says-bitcoin-suisse

[24] Op. Cit note 21 page 5

or permissionless, where anyone can enter and participate in the platform using a nickname. The most famous permissionless open/public blockchain network is the Bitcoin and also the Ethereum Cryptocurrency Network.

- **Closed-Private Blockchain Network**

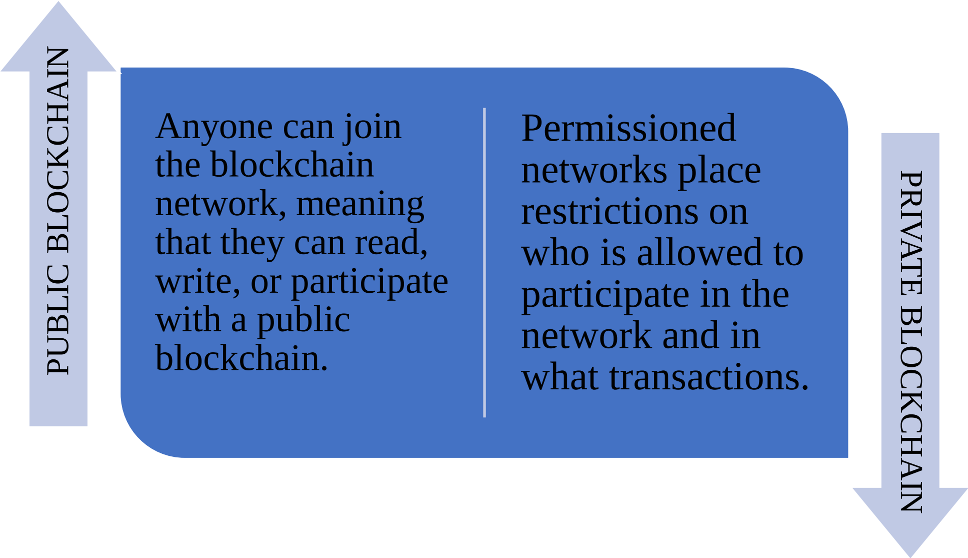
On the other hand, a private blockchain network is invitation-only and anyone who wishes to access it must ask for permission from the governing body of the blockchain. In this type of blockchain's network structure different levels of access are allowed, something that determines which users can write, read and audit the blockchain.[25]

It can also be categorized as a private permissioned enterprise, which is strictly private and the main control is in the hands of the operator or in the so-called consortium. This is a type of blockchain technology where instead of only a single organization, multiple organizations govern the platform.

In this case, organizations use the distributed ledger technology but they do not make their data public. This means that private blockchains do not offer the same level of decentralized security as their public ones and the entries can be altered by its owner. The interesting fact and the main difference from public blockchains is that private blockchains require each user to have a verified identity, since that defines the type of access they have. These are popular enterprise solutions that allow the control of the resources and actions that everyone carries out and in this way they permit faster transactions and are more energy-efficient to maintain. As a result, this facilitates much more any type of control.

Figure 2 on the next page illustrates how private and public blockchains could be categorized and some indicative examples of this categorization.

[25] (Innovation & Technology Business School, 2020)

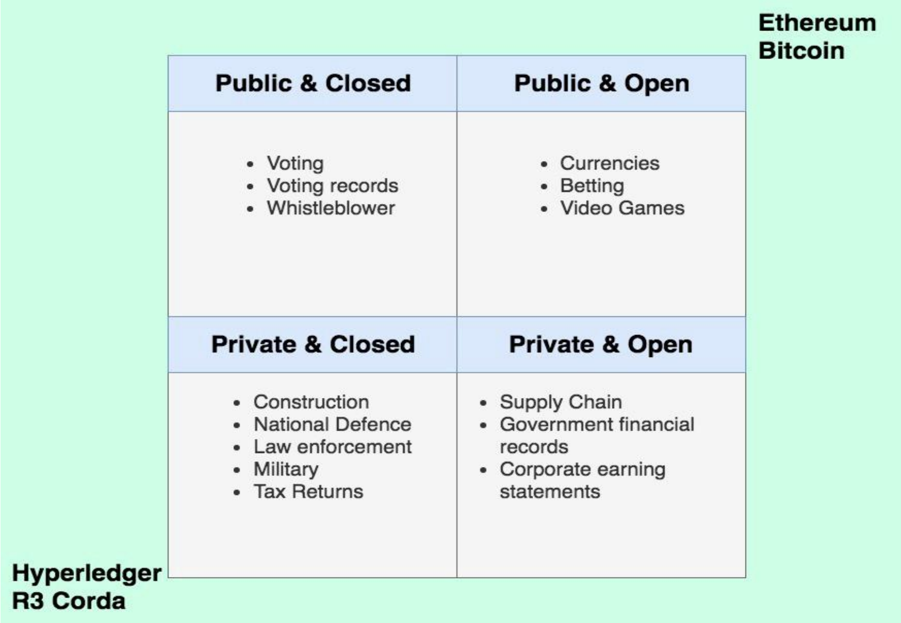


PUBLIC BLOCKCHAIN

Anyone can join the blockchain network, meaning that they can read, write, or participate with a public blockchain.

Permissioned networks place restrictions on who is allowed to participate in the network and in what transactions.

PRIVATE BLOCKCHAIN



Ethereum
Bitcoin

Public & Closed	Public & Open
• Voting • Voting records • Whistleblower	• Currencies • Betting • Video Games
Private & Closed	**Private & Open**
• Construction • National Defence • Law enforcement • Military • Tax Returns	• Supply Chain • Government financial records • Corporate earning statements

Hyperledger
R3 Corda

Figure 2. Blockchain categories and examples. [26]

The most important difference between public and private blockchains, which is connected with the issues related to Competition Law, is the role of the user on the network and how the identity of users is managed. In a private blockchain, the creator of the network knows from the beginning who the participants are. On a public network, you can't build a permission-based solution and the users have all guarantees of anonymity.

[26] Massessi, D. 2018. "Public Vs Private Blockchain in a Nutshell." Accessible at: https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f

2.4.2 Permission-less and Permissioned Blockchains

A. Permission-less Blockchains

Permission-less blockchains are blockchains that do not require users to ask for permission to join and interact with. So practically, anyone can join the network, read, write or audit the transactions without the need to ask for anyone's permission. In this form, any blockchain network may have as many validators as possible and anyone that has the right equipment can become a validator. Additionally, the identity of users is pseudonymized so that validators cannot easily identify an individual user, though anybody can observe the actions that have taken place on the blockchain between these pseudonymous parties. [27]

In this type of blockchain network it is quite hard for a violation of competition Law to appear or be identified due to the fact that any possible action of such a kind requires a conspiracy from a large group of validators. Also, it is worth mentioning that in this form, validators receive both transaction fees as well as tokens utilized as currency, in accordance with the provisions of the blockchain's protocol.[28]

It is also highly important to note that permissionless blockchains are decentralized blockchains, a crucial characteristic from a Competition Law point of view, as a result of the anonymity of the users and the transparency (with the meaning that public nodes can see the transactions any time). As a result of these characteristics the users develop a sense of trust since anyone can trace or read the transactions, plus all the data are immutable and cryptographed.

B. Permissioned blockchains

Unlike permission-less blockchains, where the anonymity and the fact that literally anyone can be part of the network and can follow up all the transactions abolishing the need of the middleman as a part of the transaction's process, in permissioned blockchains the restrictions applied on who can become a validator reintroduce the need of an intermediary. The aforementioned restrictions are introduced and applied by a controlling firm or consortia of firms, as it happens with the most private blockchain networks.

In a permission-less blockchain, access to its history is open and available to everyone. In a permissioned blockchain, however, access could be restricted to specific users (private) or even available as public information.[29] Nevertheless, in both public and private blockchains the transactions are often encrypted for privacy reasons. Near consensus requirements across validators are also often not applied, which could mean that one specific validator might be able

[27] Op. Cit note 3 pages 10-16

[28] Protocols are crucial components of blockchain technologies that enable information to be shared automatically across cryptocurrency networks securely and reliably. In the field of computing, protocols are essentially rules that define how data is allowed to be transferred between different computer systems.

[29] This distinction is crucial with the meaning that not all the permissioned blockchains are public. Libra Blockchain for example that has been developed by Facebook is a permissioned but public blockchain. The users of this blockchain are pseudonymized but transactions remain transparent and open to public.

to verify the transactions of multiple pseudonymized users. This form of blockchain network appears more suitable to facilitate behaviors that would cause violation of the provisions of Antitrust Law within the European Legislative Competition Framework.

It is the nature of permissioned blockchains that facilitates this, due to the fact that they appear more centralized, since there is a control center of the network, a smaller pool of validators coming from the ‘’controlling center’’ which might be a controlling firm or consortia of firms. This topic will be analyzed further in the next section below.

3 MAIN PART - PART B

3.1 Blockchain Technology Within the Spectrum of the European Competition Law

3.1.1 Introduction and Arising Challenges

Having in mind the aforementioned, the blockchain technology could be characterized as a simple but at the same time complex system of managing data bases. It is undoubtedly an invention that has changed profoundly the so far known and applied way of making transactions and registrations, and conducting trade. Due to fact, though, that everything about blockchain technology has been developed and grown within the last three decades, from a legislative point of view someone could spot many grey zones as to the application of law and especially the application of Competition Law.

The point is, if we want to have a closer look into the possible frictions of blockchain applications with antitrust and competition law we have to consider several anticipated blockchain applications that are discussed today. [30] Many legal and economic experts have discussed, analyzed and written articles about this topic after the rapid rise of blockchain technology, including the Competition Committee, the Organization for Economic Co-operation and Development (OECD), and the World Economic Forum (WEF). The European Commission in particular has launched several papers for discussion posing some of the following questions:

Might blockchain technology disrupt and remove the need, not only for payment intermediaries (e.g. clearing and settlement, credit cards), but also for platforms? Might blockchain technology change the nature of some firms by reducing some of the transaction costs that explain why firms do not outsource more of their activities? Should competition agencies be given permission to access blockchains?[31] Might there be potential for firms to collude through a blockchain? Might there be potential for firms to tacitly coordinate through a blockchain? Might blockchain technology be used to facilitate anti-competitive behavior? Might there be cases in which incumbents seek to prevent or delay the efficient adoption of blockchain technology? Might collaborations or consortia that set up blockchains exclude or raise the costs of rivals outside of the consortium? Might smart contracts provide a commitment device that allows firms to soften

[30] Breu, S. U. 2017. "Blockchain and cryptocurrencies challenges Anti Trust and Competition Law." SSRN Electronic Journal, January: 3-4.

[31] OECD, Directorate for Financial and Enterprise Affairs. 2018. Blockchain Technology and Competition Policy - Issues paper by the Secretariat. OECD.

price competition? Might cryptocurrencies exploit dominant positions built upon network and platform effects by charging excessive transaction fees? Might third parties exploit or exclude using a dominant position that depends upon blockchain related demand? Might the principles of competitive neutrality be breached, and hence competition distorted, by policies that disadvantage or favor those firms that use blockchain technology?

Dr. Thibault Schrepel, Assistant Professor, Utrecht University School of Law and Faculty Associate, Harvard University's Berkman Klein Center, in his article ''The theory of Granularity'' tries to analyze which is the role that each participant or group of participants plays in the context of horizontal governance of public permissionless blockchains. His approach is that once we identify the ''blockchain nucleus'' as he names it, which is practically the subjects participating in Blockchain more actively and then someone could assume that in a way they control the network.[32] In this case antitrust and competition law becomes applicable again, since this determination of nucleus allows to identify the relevant market, the market power and to assign liability.

According to his approach, in the first part of his article, Schrepel presents how the fundamental concepts of antitrust law are highly connected with the theory of the firm as presented and defined by Ronal Coase[33]. He specifically underlines that this theory '' is at the heart of modern antitrust and competition law'', due to the fact that based on this theory, we can successfully point out where, how and from who control is exercised and having this in mind define the limitations of firm's activities that they might threat to violate competition law's provisions.

As public permissionless blockchains are open to everyone and no further action is needed for anyone to access, make transactions and exit them, one should question the applicability of competition law in an entity of such type, that resembles to nothing to the economic entities that has so far concern competition law.

In the second part of his article, Schrepel provides an analysis trying to answer the following question: To what extend a blockchain could be used to facilitate organization of economic activities outside the concept of the firm as mentioned above, outside the concept of undertaking as defined by anticompetition legislative framework in a way that twist and turn the application of antitrust policy on its activities?

After having defined blockchain technology as a new institution regarding transactions and having shown that in this new way of transact there cannot be found objectively and with the so far used techniques and definitions market power nor command control, something that leads to twist and turn of the antitrust and competition law. Then, what is left in his opinion, is to determine to which extent and in which manner antitrust and competition law can be applied to these platforms and to what extent and in which manner this platform may use their nature in order to avoid such an application.

[32] The Theory of Granularity: A Path for Antitrust in Blockchain Ecosystems, Thibault Schrepel, University Paris 1 Panthéon-Sorbonne; VU University Amsterdam; Stanford University's Codex Center, Page 36, 29 Jan 2020

The explanation is simple: ‘’It appears that blockchain is a new institution that does present similar characteristics to those of the firm. To the extent that antitrust and competition law relies on these features, they become mostly inoperable in the face of blockchain. The bigger blockchain will get as a transactional institution, the bigger the problem will be. A new theory must be found so to create a new legal fiction to which the law can be (re)applied’’.[34]

Stefan Urs Breu in his article ‘’ Blockchains and Cryptocurrencies challenging Antitrust and Competition Law’’, also presents his perspective about blockchain technology and the possible frictions of blockchains with Antitrust and Competition Law. He raises important questions about the future of blockchain technology further indicating the wide range of grey zones in regards to the application of competition law.

Legal and economic experts have noticed, discussed and defined the problems that have been raised when it comes to the application of Competition Law and actions needed to be taken by the competition authorities on blockchain platforms. Best efforts notwithstanding, however, there have not been sufficient, complete and final answers yet. Blockchains and cybercurrencies are driving a challenging new development period for legislative regulations and law enforcement in general but antitrust and competition law in particular.[35] There is a wide range of potential problems from the application of the so far known antitrust law when it comes to platforms and undertakings using blockchain technology.

In the following sections of our project we will consider how the rise of blockchain technology is relevant to the work of competition authorities. There are plenty of questions arising as to the effect of blockchain technology on matters such as access to data, collusion, abuse of dominance position, competitive neutrality and much more. There is a number of potential topics for discussion, some interesting approaches of how this interaction should take place, conclusions and proposals for the best possible co-existence between Law, Economics, and blockchain technology within the European Legislative Framework Regarding Competition Law.

3.2 European Competition Legislative Network

3.2.1 Treaty of functioning of European Union Article 101[36]

The use of blockchain technology can raise antitrust issues, but the nature of these issues does not appear different in kind from similar issued raised by any other business conduct.[37] In this base, it is obvious that companies which implement blockchain solutions fall under the application scope of the European Competition Legislative Framework. It is also known that the blockchain technology has attracted considerable interest from antitrust authorities over the last years. The question arising here is whether the anti-trust authorities can actually investigate, find and punish such violation of Competition Law and how these actions can take place effectively.

[34] Op. Cit note 30 page 3-5
[35] Op. Cit note 30 page 3
[36] European Commision, Consolidated version of the Treaty on the Functioning of the European Union - PART THREE: UNION POLICIES AND INTERNAL ACTIONS - TITLE VII: COMMON RULES ON COMPETITION, TAXATION AND APPROXIMATION OF LAWS - Chapter 1: Rules on competition - Section 1: Rules 2008
[37] Matthias Artzt, Handbook of Blockchain Law: A Guide to Understanding and Resolving the Legal Challenges of Blockchain Technology, 2020 pages 15-21

Plus, can Blockchains complement antitrust law in realms where the latter is inapplicable or under forced?

To answer these questions and many other that are extensions of this concept we should first better provide a brief introduction to the relative provisions by the Treaty of Functioning of the European Union (TFEU). More specifically Art. 101 (1)[38] of the TFEU provides the following:

All agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market, and in particular those which:

a) Directly or indirectly fix purchase or selling prices or any other trading conditions
b) Limit or control production, markets, technical development, or investment
c) Share markets or sources of supply
d) Apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage
e) Make a conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.

Agreements, decisions and concerted practices (collectively, agreements) that are caught by Article 101(1) TFEU are automatically void under Article 101(2) TFEU unless they yield competitive benefits recognized in Article 101 (3) TFEU:

Agreements, which contribute to improving the production or distribution of goods or to promoting technical or economic progress while allowing consumers fair share of the resulting benefit, and which (do) not:

a) Impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives
b) Afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question.

Thus, the prerequisites for the application of Art.101 (1) are the existence of an ‘’agreement’’, ‘’concerted practice’’ or ‘’decision’’ involving multiple undertakings that they might have an anticompetitive object or effect within the EU. In order to move forward with this analysis, it would be useful to briefly define the above terms.

Speaking of agreements, we refer to decisions and concerted practices and we can interpret broadly this term so that includes both formal and informal agreements. It is quite hard though to define whether or not a conduct consists an agreement that falls within the above definition. The reason why is that in Blockchains it is quite hard to distinguish between legal tacit collusion, in the meaning of parallel but independent actions taken within blockchain Network and Illegal coordination, where coordinated action has taken place leading to violation of the provisions of the Article, as a part of a big plan.[39]

[38] Op. Cit. Note 36 page 1
[39] Capobianco, A., and Pike, C. 2020. Antitrust and the trust machine. OECD Blockchain Policy Series. Accessible at : https://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf.

As to the term undertaking it is known that includes in the spectrum of European Competition Law any kind of enterprises, business organizations, companies and even individuals. In Blockchain platforms same interpretation of this term should be applied including also validators, users and sometimes developers.[40]

Another fundamental distinction is made between the so-called horizontal agreements among head-to-head competitors and so-called vertical agreements among companies at different levels of a supply chain. As a general rule, horizontal agreements are viewed more negatively from an antitrust perspective, while vertical agreements are considered less likely to raise antitrust issues. However, the application of blockchain technologies can raise antitrust issues in both horizontal and vertical agreements.

Article 101(3) can be applied in individual cases or to categories of agreements and concerted practices through block exemption regulation. Plus, the guidelines focus on individual cases and provides for each of the 4 conditions to satisfy Article 101(3) indications as to how they will be applied. Thus, an agreement can be permitted if contributes to improving production or distribution of goods or generally promotes technical or economic progress, if consumers receive a fair share of the resulting benefits, if the restrictions posed could be characterized as essential in order to achieve these objectives and last but not least if the agreement does not give to the agreed parties any possibility of eliminating competition in respect of substantial elements of the products in question.

Easily someone could conclude that agreements coming from parties working within the Blockchain Network could easily fall under the application scope of this provision and in fact it is in many cases the nature of Blockchain Technology and Network that leads towards this direction. It is worth mentioning that some of these agreements may be permitted as an exception under the paragraph 3 of Art. 101, which acknowledges that some restrictive agreements may generate objective economic benefits that outweigh the negative effects of the restriction of competition, and exempts those agreements from these prohibitions.[41]

3.2.2 Treaty of Functioning of the European Union – Article 102

Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States.

Such abuse may, in particular,[42] consist in:

a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;
b) limiting production, markets or technical development to the prejudice of consumers;

[40] There will be a brief analysis of the role of the participants of a blockchain network and how they can maybe influence the network

[41] European Commision, Guidelines on the application of Article 101(3) TFEU (formerly Article 81(3) TEC) 2020)

[42] Blockchain the DMA & DSA, presentation P.P National & Kapodistrian University of Athens, DR. Dionisios Pelekis

c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.

Article 102 applies only in case that there is an abuse of a 'dominant position'. The dominant position itself is not -and it shouldn't be punishable by the provision. This dominant position should be obvious within the European Union or a substantial part of the European Union by an undertaking, as the meaning of undertaking was discussed above. Also, in order this provision to be applied it is required that the abuse of dominant position should affect trades between Members States.

Article 101 TFEU can address anti-competitive agreements and concerted practices between companies, while Article 102 TFEU can address the exploitation of a dominating position by a company. Some structural competition issues, however, are outside the reach of EU competition legislation or cannot be handled effectively.

In order to define when an undertaking actually holds a dominant position based on decisions or opinions of the European Court of Justice, somebody should take into consideration the following factors: 1) the product market, 2) the geographic market. After these factors have been well defined and considered there is need to examine the company's market power in these two. As to how a relevant market is defined when it comes to antitrust law is usually critical to the European Courts' analysis and justification and so goes regarding dominant position.

Such an approach to market definition is outlined in European Court's notice in 1997 on the definition of the relevant market for the purposes of Community competition law. According to this notice, the exercise of market definition consists in identifying the effective alternative sources of supply for the costumer of the undertakings involved, in terms both products, services and of geographic location of suppliers.

3.3 Consensus Mechanisms and Participants of a Blockchain Network from a Perspective of Anti-monopolistic Legislation

To start with the first topic that raises a lot of questions is -as mentioned above, the potential of violation of competition law provisions, due to consensus mechanisms used in blockchain networks.

In fact, there are three different groups that might have the power to organize a cartel or a dominant position (and potential abuse of this position): the miners (including validators), the programmers and the users. This should be taken into consideration from the perspective of anti-monopolistic legislation while shaping relative legislative framework or guidelines.

3.4.1 Miners[43]

Let's start our analysis with miners. Mining, as it was already explained above in the first part of this project, is the procedure of adding blocks in an already existing blockchain. In broadly used blockchains, a great number of transactions is added every day and so, the power of each miner is quite limited. Nevertheless, the situation is different when a lot of miners create a pool - the so-called mining pool, where the profit by their activity is divided pro rata based on the computer power that each of them offers to the pool. The motive for the miners to join these casts leads to very powerful extensions under the spectrum of competition law.

As a result, less than 10 pools managed to be dominant in Bitcoin platform in 2017. In fact, the seven most powerful teams were responsible for more than 85 % of all the transactions that were verified in Bitcoin's blockchain.[44] This could raise doubts regarding the major advantage of this technology, which is not other that its decentralized character, since (in this example) the control in a percentage above 51% of the sum of the participants in the verification procedure practically means the control of the blockchain. Practically only a change in the consensus mechanism of the blockchain could redivide the mining power.

The consensus mechanisms are different as to the way of data verification, but not that different as to the way with which the users can read/access information and add new transactions. Thus, is the integrity of the blockchain that is on stake and not its function. For this reason, none of the consensus mechanisms could be considered as anticompetitive by itself, but many of them tend to facilitate the existence of anticompetitive practices. In contrast with practices, whose results appear out of the blockchain, this type of potential collusion produces effect only within the blockchain, reducing significantly the detection risk.

As a result, the competition authorities should be alert to detect the chances of anticompetitive behavior in different consensus mechanisms. The point is different consensus mechanisms present different number of chances as to the potential existence of anticompetitive practices.

3.4.2 Proof of Work (PoW) and mining[45]

As already exposed above, the consensus mechanism of proof of work gives the miners the opportunity to compete with each other as to who is going to first add a sum of transactions – concentrated in a block- in the blockchain by solving a cryptographic puzzle. The first who is able to solve the puzzle gets as a reward a transaction fee as well as newly formed currencies, tokens. Due to the Bitcoin's recognition in a global scale, this is the most famous verification mechanism. The PoW mechanism has the advantage that it allows a relatively random allocation of the verification that limits the chances of collusion.

[43] Op. Cit. Androtsopoulou note 5 , page 33

[44] BLENKINSOP C., Blockchain 's Scaling Problem, Explained, Cointelegraph, August 2018.

[45] Op. Cit. note 5 pages 30-33

3.4.3 Proof of Stake (PoS)[46]

PoS as consensus mechanism works a bit differently. The chance of a user to be the one that he will be involved in the verification of a block are analogous of the number of the cryptocurrencies that he holds in the system or their antiquity. Given the fact that in this case there is no mining procedure taking place, there is also no introductions of new coins into the system and so the validations taking place are remunerated exclusively with fees on the added transactions. The number of validators depends on the system. In any case the validators have nothing on stake and can create arbitrarily more blocks so they can receive biggest rewards.

This matter of integrity is highly important for the anti-monopolistic legislation because the assurance of this integrity it is up to the most powerful users. Thus, anticompetitive practices are more likely to appear in this system in comparison with the Proof of Work mechanism.

3.4.4 Proof of Activity[47]

Proof of Activity is a combination of the aforementioned consensus mechanisms. The miners are competing in solving the cryptographic puzzle as in PoW system. The formed blocks though do not contain transaction, they function as a template, a pattern. This system also uses Proof of Stake mechanism. A random team of validators is chosen to validate the new block. The more tokens somebody holds the more likely is to be chosen to validate the transaction. The fees in the system are shared between the miners and the validators. Thus, this consensus is more likely to encourage illegal agreements between users having high efficiency computer systems and users having many tokens. [48]

3.4.5 Proof of Burn

Proof of burn is mechanism in which the users ‘’burn’’ currencies or marks by sending them in an address where they can not be recovered. The more coins or marks a user burns, the more likely it is to be chosen to create new blocks. The integrity of this procedure is in this case on the hands of the most powerful users of the blockchain and so the chances of collusions are higher, since these ‘’powerful players’’ are in position where they can actually perform effective control in the certain blockchain. As a result, the existence of anticompetitive practices in facilitated.

3.4.6 Proof of Capacity

In Proof of Capacity what matters is the amount of free space a user has in its hard drive. The more space a user has the more is likely for him to be chosen as a validator. Also, in this

[46] Op. Cit note 8 page 53
[47] Op. Cit Androtsopoulou note 5 page 34
[48] Op. Cit note 5 pages 48-52

system the power is on the hands of those who have more resources, giving the opportunity and the motive for the appearance of anticompetitive agreements.

3.4.7 Proof of Elapsed Time

In this consensus mechanism the users do not have to solve a cryptographic puzzle, but the algorithm uses a system of reliable execution in order to secure that the blocks are created in a way that resembles more to a lottery, with'/out any work coming from the combination. This system is similar to PoW but consumes way more less electric energy. The randomness in the selections of the users who are responsible to validate the blocks reduces the risk of collusive agreements.

Given the analysis of the different consensus mechanisms as they were exposed above, we can conclude to some points regarding the possible appearance of anticompetitive behaviors from the side of the miners. This possibility is high in cases where miners and validators are ''big players'', within the meaning that the users that are in a powerful position can possibly set in doubt the integrity of the whole system. Plus, since this power is recognized by the broader community, the risk of briberies emerges for the accomplishment of their own interest.

On the contrary, the risk of collusion is reduced significantly when the selection of validators is random. Up to today the two most powerful blockchain platforms, Bitcoin and Ethereum, use the mechanism Proof of Work which minimizes the risk of contracting of anticompetitive agreements. Nevertheless, the developments in the field of blockchain technology are rapid and incessant with all of these data to be altered on permanent basis. So, for example the Ethereum platform is about to change in Proof of Stake consensus mechanism and this can maximize the potential risks from a competition law point of view. In any case competition authorities should stay aware regarding the special characteristics of each system and give the due attention mainly in the cases when the way for violation of competition rules is favorably paved.

3.4.8 Programmers

The programmers working on basic software of blockchain constitute small groups with great power within the network, since they are the ones that develop the official software on the basis of which the whole system renders functional. This occurs for example in case of Ethereum Foundation and Bitcoin Foundation whose mission is the promotion of their blockchain protocol. The Bitcoin Foundation cooperates also with third parties such as the MIT Digital Currency Initiave, the Blockstream and the ChainCode Labs for the development of blockchain. The same applies to private blockchains such Hyperledger and R3 since they are not open sources and they have corporate members to finance them and contribute to the formation of their code.

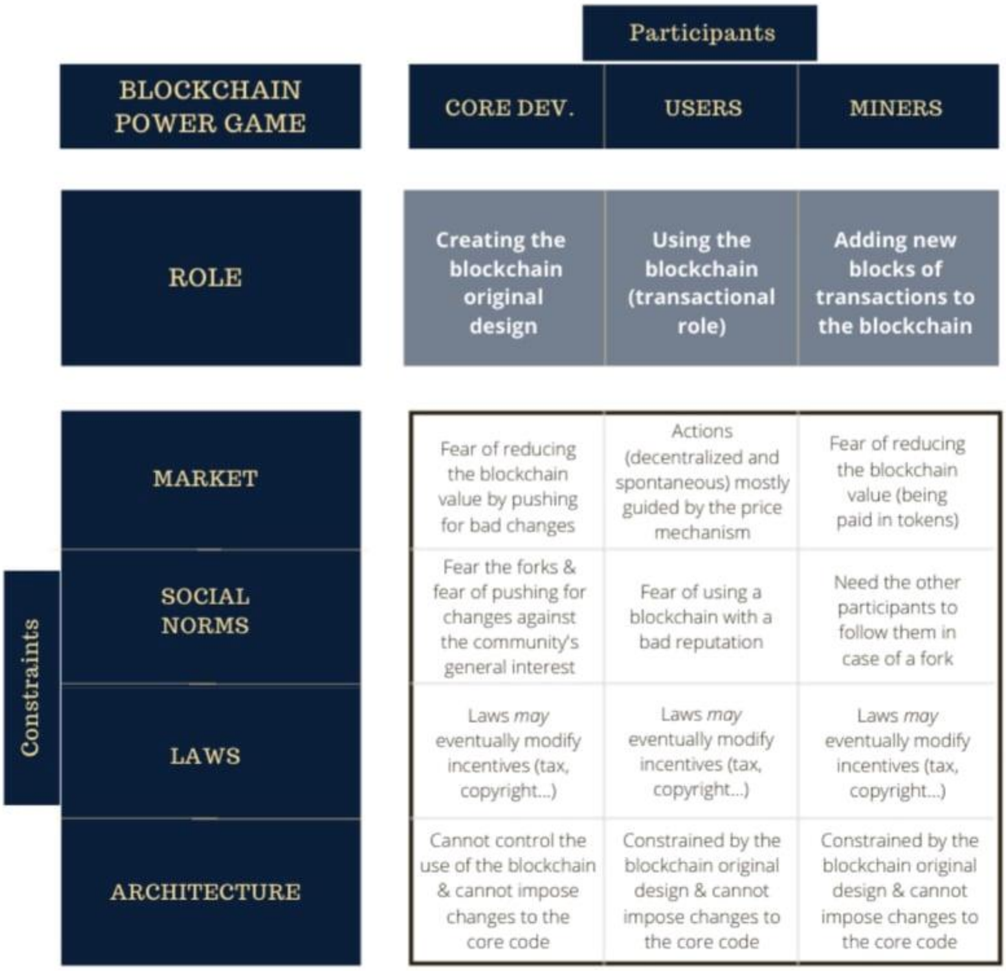
The programmers should also come in contact with the miners. The Bitcoin uses a mechanism named BIP 9, that allows the programmers to communicate with miners concerning technical changes. In private blockchains the owners or certain participants they have the power to resolve disparities in the chain that they cannot be resolved on the basis of an objective consensus mechanism, but require unilateral intervention. Such cases obviously lead in control of the blockchain which gives a bust to potential collusion.[49]

3.4.9 Users[50]

Also, collusive agreements can appear by certain users of the blockchain. Apart from each consensus mechanism that can facilitate more or less agreements between miners or/and validators management mechanisms existing in the blockchain, which the allow the users perform binding voting for changes in the network. These are likely to give bust in agreements between miners and /or users. Generally depending on the consensus mechanism applied, the possession of a great number of marks/coins can empower the imposition of decisions or the coordination with other powerful users. In Bitcoin platform 1000 persons hold the 40% of the whole market. This is often referred to as ‘’Whale problem’’ and obviously the Bitcoin Platform is not the only one who deals with this.

[49] Op. Cit. note 21

[50] G. Kalogerakis, Nikolaos I. Theodorakis, Blockchain: Implications, Potentials and Challenges for the Greek Legal System, DIMME, Issue 1 page 9



	BLOCKCHAIN POWER GAME	Participants		
		CORE DEV.	USERS	MINERS
	ROLE	Creating the blockchain original design	Using the blockchain (transactional role)	Adding new blocks of transactions to the blockchain
	MARKET	Fear of reducing the blockchain value by pushing for bad changes	Actions (decentralized and spontaneous) mostly guided by the price mechanism	Fear of reducing the blockchain value (being paid in tokens)
Constraints	SOCIAL NORMS	Fear the forks & fear of pushing for changes against the community's general interest	Fear of using a blockchain with a bad reputation	Need the other participants to follow them in case of a fork
	LAWS	Laws *may* eventually modify incentives (tax, copyright...)	Laws *may* eventually modify incentives (tax, copyright...)	Laws *may* eventually modify incentives (tax, copyright...)
	ARCHITECTURE	Cannot control the use of the blockchain & cannot impose changes to the core code	Constrained by the blockchain original design & cannot impose changes to the core code	Constrained by the blockchain original design & cannot impose changes to the core code

Appendix n°1: A representation of blockchain power game

Figure 3. Participants of a Blockchain Network.

4. Anticompetitive Agreements

Anti-competitive agreements are undoubtedly one of the most discussed, controversial and highly connected with the EU competition policy issues. Section 3 of the Competition Act (2002) and Art. 101 TFEU, prohibits enterprises, persons, or association of enterprises (or persons) from entering into anti-competitive agreements related to production, supply, distribution, storage, sale (or price), and trade in goods or provision of services. Specifically, the Act restricts a firm (or association of firms) from colluding with other firms (or association of firms) at the same or different levels of the production chain. [51]

[51] See above part A article 101 TEUF

In this section we will try to analyze and discuss the potential examples of anti-competitive agreements[52] (based on current available information relating to blockchains) and how they may be addressed within the purview of the existing law. It is first useful to keep in mind that, as already analyzed above, EU competition law prohibits all forms of restrictive agreements and concerted practices between companies.

4.1 Horizontal Agreements and Information Exchange

Horizontal agreements are restrictive agreements between competitors that operate at the same level of the production/distribution chain. Horizontal agreements that have as their objective or effect or likely effect the prevention, distortion or restriction of competition directly or indirectly constitute *per se* violations.[53]

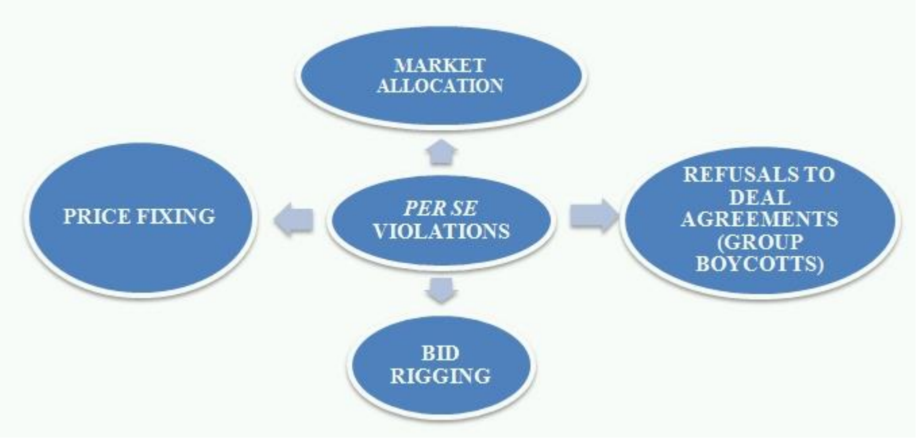


Figure 4. Violations in horizontal agreements. [54]

In the case of competitors (firms engaged in the same economic activity), anti-competitive agreements often take the form of collusion (cartelization or bid rigging[55]). Various efficiency reasons may exist for competitors being a part of the same blockchain application (such as the creation of a new market or improving the current processes). However, in certain cases, blockchain applications can also alter the gains and challenges associated with maintaining a collusive agreement.[56]

For a collusive agreement between competitors to be successful, the firms that are a part of such an agreement should be able to:

- Interact with each other and arrive at a mutually agreeable coordination strategy.

[52] According to the term ‘’agreement” includes any arrangement or understanding or action in concert, (i) whether or not, such arrangement, understanding or action is formal or in writing; or (ii) whether or not such arrangement, understanding or action is intended to be enforceable by legal proceedings.

[53] European Comission. 2021. "Revision of the two Block Exemption Regulations for horizontal cooperation."

[54] Elig Gurkaynak. 2020. Horizontal Agreements. Accessible at: https://www.mondaq.com/advicecentre/content/1548/Horizontal-Agreements

[55] Bid rigging is an illegal practice in which competing parties collude to determine the winner of a bidding process.

[56] Op. Cit. Pelekis note 42 page 13

- Monitor each other’s conduct to ensure adherence to the agreement.
- Punish a firm in case of deviation from the agreement in such a way that the penalty supersede the benefit from cheating on the collusive agreement.

The question is how the use of blockchain technology could facilitate such behaviors? Let’s use as an example the exchange of information within a blockchain network.[57] One of the benefits of blockchain is the ability of creating trust through a repository of verified immutable records. Blockchain applications facilitate sharing of a large amount of information, thereby increasing transparency. Transparency of information generally is expected to intensify competition. However, in some cases, it is possible that there may be visibility of information belonging to competitors, who are part of the blockchain. In a blockchain application, unless adequate measures are adopted, the transactional information in the ledger can be easily viewed by the blockchain participants, the so-called ‘’visibility effect’’.[58]

Although the same information may not be accessible to entities outside the blockchain (opacity effect) due to restricted access (in case of a permissioned consortium blockchain) or encrypted data with pseudonyms (in case of a permission-less public blockchain). Adequate safeguards should be put in place to ensure that this feature does not enable competitors to arrive at an agreement and monitor each other’s conduct. However, it is important to consider whether there is any difference that blockchain applications create for information exchange vis-à-vis other existing systems (such as physical or digital exchange of information). One difference may be that through a blockchain information can be exchanged on a near real-time basis. Additionally, there may be greater trust in the authenticity of the data stored in a blockchain than other systems, due to the secure and immutable nature of blockchains.[59]

In general market uncertainty and volatility reduce chances of a stable cartel, since the participants of the cartel cannot differentiate between market volatility and competitors’ behavior causing such volatility in their own performance. However, when most players participate in a blockchain application, the resulting transparency in market information may reduce such uncertainty. For example, if each participant has information about the total number of transactions taking place on the blockchain application, it may provide an accurate and real-time indication of market conditions to the participants of a collusive agreement. This may allow them to differentiate between the instances of poor market conditions and deviation from the cartel agreement**.**

To conclude, in the first sight it would be incorrect to assume that blockchain applications always facilitate collusion. But such a possibility may exist when competition-sensitive information is shared among competitors. Competition-sensitive information includes information about current and/or future price, discounts, profitability, cost, production, or information on future

[57] Exchanges of information are interactions among competitors that, from a competition law perspective, may fall between the universally condemned hard-core “naked” cartels and tacit collusion arising from oligopolistic interdependence, generally considered legal.

[58] Competition Comitee of India. 2021. "Discussion paper on Blockchain Technology and Competittion.", page 22

[59] Matthias Artzt, Handbook of Blockchain Law: A Guide to Understanding and Resolving the Legal Challenges of Blockchain Technology , 2020 page 21

strategy and investment plans. Generally, sharing of data not related to price, cost or output and historic or aggregated data, do not raise concerns with respect to competition law.

However, blockchains record transaction data, which may include competition sensitive data on quantity and price. Further, since new blocks are added to a blockchain without significant delay, the data is also not historic (and is shared frequently). Concerns are less likely in the case of blockchain applications that include only the information that must be communicated to achieve their defined objectives and exclude other competition sensitive information which can be used for unlawful information exchange. For instance, in a blockchain application whose focus is to record land ownership, the only data that should be ideally recorded and shared should be the sale of land from A to B and not its price.

Governance rules of some blockchains, such as Corda[60], are designed such that when a transaction takes place, only the minimal and required amount of information is recorded in the blockchain. Thus, just like industry associations, blockchains also need to avoid certain conduct. Specifically, a blockchain should undertake all necessary measures to ensure that competition sensitive data is not shared among competitors.

4.2 Vertical Agreements

Vertical anti-competitive agreements take place between firms engaged in different stages of the value chain, and could take the form of tying-in agreements, exclusive supply/distribution agreements, refusal to deal agreements, and agreements aimed at resale price maintenance. The Section 3(4) of the Act and Art. 101 TFEU refers to this type of agreements and intents to describe the forms in which they may appear.[61]

Generally, in the context of operating of a Blockchain network someone could support that those vertical anticompetitive agreements are more likely to happen in comparison to horizontal agreements, a claim that will be analyzed in the following paragraphs. Above are some possible types of vertical agreements, as they could possibly take place through a blockchain network:

- A blockchain’s governance prohibiting access for an entity using a competing blockchain application/wallet/exchange.[62]
- An agreement between a blockchain platform and developer of blockchain applications running on the platform prohibiting/restricting the developer from dealing with any other competing platform.
- An agreement by a mining hardware provider tying the sale of its product to a miner by using a specific wallet.

[60] Corda is an open source blockchain-based distributed ledger technology and smart contract platform operating on a decentralized global network. It is designed to record, manage and automate legal agreements between business partners.

[61] THE COMPETITION ACT, 2002, Act of Parliament, received the assent of the President on the 13th January, 2003, chapter 2, page 5.

[62] This type of conduct is referred as exclusionary practice and it will be analyzed more below as a form of abuse of dominant position.

- An agreement between a blockchain and its nodes/wallet/exchange that requires the latter to use only the blockchain application in question (thereby prohibiting the latter from participating in any other competing blockchain application).
- Smart contracts that self-enforce tie-in, exclusive supply/distribution, refusal to deal, or minimum resale price maintenance between entities at different levels of the value chain.[63]

In some cases, the above vertical agreements could adversely affect the competition. Whether a vertical agreement is anti-competitive or not, is assessed on a case-by-case basis by balancing the anti-competitive impact against justifications for the vertical arrangement. While analysis is undertaken on a case-by-case basis, generally the vertical anti-competitive agreements have a higher probability in the case of permissioned consortium blockchains than permission-less public blockchains. If a public permission-less blockchain, already in operation, is to engage in a vertical restraint such as a refusal to deal with an entity, there is a need to modify its rules, which would require the nodes to be in consensus with each other. Further, any such change in a public permission-less blockchain's protocol would imply that it is no longer "permission-less" and "public".

In a permissioned consortium, however, blockchain nodes can adjust their governance rules to engage in such behavior (by denying an entity access to the blockchain's information, banning them from proposing new transactions, and prohibiting them from confirming transactions). In a public blockchain, there is no incentive for the blockchain application to impose an exclusive dealing condition for the publishing of blocks because the data is public. Furthermore, given the fees involved, the node has no motivation to publish the block in another public blockchain once it has been published in the first.[64]

In a permissioned blockchain, however, dealing solely may appeal to a blockchain application if it seeks to be the only source of data on a transaction (being the only source of data may boost the blockchain's attractiveness). Blockchain technology has the potential to offer a number of market efficiencies and pro-competitive outcomes. For example, a factory using blockchain technology to manage input procurement may be able to explore a wider range of suppliers due to the increased confidence produced by the blockchain system. This could lead to more competition, which would benefit consumers.

Some blockchain technology innovation may be viable only on permissioned blockchains with appropriate and justifiable access limitations. To summarize, there are a variety of efficiency reasons why businesses may prefer a permissioned blockchain over a permission-less and public blockchain, and these considerations are taken into account when doing a competitive analysis.

4.3 Risk of Collusion and risk of Monopolization: The Libra Case

Dr. Thibault Schrepel,[65] also published in April 2020 another paper in which he specializes

[63] Tying is an agreement by a party to sell one product but only on the condition that the buyer also purchases a different (or tied) product. There will be a brief analysis of tying policy in blockchain in the next Chapter.
[64] Op. Cit. note 30 page 28
[65] Schrepel, T. 2018. "Is Antitrust Law Doomed by Blockchain? The antitrust Paradox." Pages 281-287

some of the questions set from his aforementioned article as well as from other legal experts under the title ‘’Libra: A Concentrate of "Blockchain Antitrust"’’.[66]

In this paper the author develops some thoughts and comes to some conclusions while using Libra as an example of a project that shows the challenges that are arising out of a competition law perspective from the use of blockchain technology.

Specifically, he claims that the Libra initiative poses a slew of antitrust issues, something that is not surprising given the scope of the project.

To begin with, in this platform anticompetitive activities would have an impact on many billion users. The stakes are high, as they are for any firm that sells a product or provides a service that is used all over the world.

Also, anti-competitive practices could become unstoppable if they are conducted on a blockchain. The Association[67] will lose all revocation power on a number of practices even if Libra is permissioned, which calls into doubt its immutability. [68]The Association will need the agreement of a majority of its nodes to change the consensus process. Anticompetitive behaviors linked to the consensus will be more difficult to stop as the Association grows in size.

Third, even after taking into account the aforementioned issues, the European Commission's decision to send a questionnaire to Libra before to its official launch is unusual. Antitrust agencies are responsible for resolving market failures. Such failures do not occur here yet, by definition—Libra is still a work in progress.[69] As a result, the European Commission's inquiry to look into "possible anti-competitive activity" appears to suggest that political elites are concerned about the expanding influence of technology behemoths. Antitrust law-related interrogations do not apply to all projects in the pipeline.

Finally, Libra's introduction to the cryptocurrency world must not be overlooked. Even if it denies it, the Libra Association seeks to compete with state currencies and the existing financial system.

The European Commission is sending a strong signal about its preparedness to initiate investigations the day Libra launches by sending out a questionnaire at such an early stage of development. The United States has also issued similar signals. These actions raise worries about whether national antitrust authorities' adversarial attitude will ultimately discourage the entrance of new competition in the bitcoin area, resulting in the retention of current regulatory, political, and economic conditions monetary power structures [70]. More broadly, such early mistrust by

[66] Libra is a cryptocurrency created by Facebook. The Libra cryptocurrency is intended to be used as a simple, low-fee global currency. It will essentially be digital money on your phone, which can be used to pay for any purchase where the cryptocurrency is supported. Libra is backed by a basket of assets, including major currencies and government debt instruments.

[67] We are referring to Libra’s Association

[68] Thibault Schrepel, Antitrust Without Romance, 13 N.Y.U. J.L. & LIBERTY (forthcoming 2020)

[69] For an empirical study documenting how antitrust officials may protect their own interest rather than the interest of the greater population, see Schrepel, supra note 50. Also, see Aurelien Portuese & Julien Pillot, The Case for an Innovation Principle: A Comparative Law and Economics Analysis, 15 MANCHESTER J. INT’L ECON. L. 214 (2018) (arguing that following a precautionary principle is causing negative effects on innovation).

[70] See Danny Nelson, FTC Commissioner Cites Libra in Support of Fed’s Real-Time Payment System, COINDESK (Nov. 8, 2019), accessible at : https://www.coindesk.com/ftc-commissionercites-libra-in-support-of-feds-real-time-payment-system [https://perma.cc/P7GW-TCG3?type =image

international antitrust agencies raises doubts about the agencies' ability to intervene impartially; after all, Libra would compete with the government's own products.

As a result, the antitrust agencies' motivation to intervene is influenced. As cryptocurrencies become more popular and mature, these terms will become more common. On a worldwide scale, regulatory issues will continue to abound the legal framework. [71]

5. Abuse of Dominance (Section 4 of the Act, Art 102 TFEU)

The Act and especially the art.102 TFEU forbids an organization from exploiting its dominating position in a relevant market, in addition to anti-competitive agreements. The market strength (or dominance) of the company under inquiry, as well as the influence a dominant corporation's activities which may impact competition, are all factors to consider when assessing competition linked to abuse of dominance. [72] Blockchain raises important questions about what a dominant position is. Because decentralized organizations like blockchain are not recognized as legal persons, many issues arise, such as: “Can a non-entity hold a dominant position?” Can blockchain create a “monopoly without a monopolist?”[73]

5.1 Calculation of Market Shares

Konstantinos Stylianou Associate Professor at University of Leeds School of Law and Nic Carter, Co-founder, Coin Metrics Partner, Castle Island Ventures in their article on Journal of Competition of Law and Economics tried to give an answer to what would be a proper calculation of market shares when in come to blockchain Platforms.

In their paper they present some thoughts about inter-asset and intra-asset calculation. In the following part of this project, we will expose some of their thoughts while trying also to give answer to the issues arising regarding the calculation of market power in cryptoassets markets.

Although some rules and obligations apply uniformly to all economic actors in a given sector, many others, such as antitrust laws and some financial regulations, as well as investor decisions, are influenced by the relative economic size of those actors, meaning that those with larger market shares can become more attractive regulatory or investing targets. As a result, adequately measuring the economic impact of economic actors in the crypto economy is a core issue, as otherwise regulatory supervision and investor decisions may be deceived.

For a variety of reasons, including unfamiliarity with the underlying technology and roles of relevant actors, there is a lack of comprehension of the economic relevance of the applicable metrics, and the unreliability of self-reported statistics, which is aided by a lack of regulation. The following paragraphs are focused on the first systematic examination of the economic footprint of

[71] LAWRENCE LESSIG, CODE: VERSION 2.0, at 8 (2d ed. 2006) (“We are at a stage in our history when we urgently need to make fundamental choices about values, but we should trust no institution of government to make such choices.”

[72] European Comission 2002

[73] Op. Cit. Note 3 pages 4-9

crypto assets and their constituent actors —mining pools and crypto exchanges—recognizing the importance of crypto asset size in a number of regulatory and policymaking areas and the fact that previous attempts have been incomplete, simplistic, or even plainly wrong.

We want to accomplish a lot of things: to introduce, identify, and organize all relevant and meaningful metrics of crypto economic actors market share calculation; to develop associations between metrics and explain their meaning, application, and limitations so that it is clear in which context metrics can be useful or not, and what the potential caveats are; to develop associations between metrics and explain their meaning, application, and limitations so that it and to show measures and their utility in assessing the proportions of crypto economic actors in their respective marketplaces using extensive, curated, and vetted data. So, in the following paragraphs we will try to present a complete and understandable picture of the crypto-economy scale and present some of the ways that we could actually evaluate the position that a a blockchain network might hold in the relevant market.[74]

5.2 Market power evaluation

As mentioned above, one of the keys in order to define anticompetitive behaviors is the determination of the relevant product and geographic markets, followed by an examination of market power (dominance) in the delimited relevant market. It is the first step in evaluating an allegation of abuse of dominance (or analysis of a proposed combination). Market power analysis is critical because it allows investigators to rule out scenarios where the firm under investigation is a small player whose actions are unlikely to undermine market competition. Product market that is relevant and the demand substitutability of the product/service is crucial principles used to define the relevant market.

According to art. 102 TFEU and to the Act[75], a "relevant product market" is defined as a market that includes all items or services that the consumer considers interchangeable or substitutable due to product or service qualities, prices, or intended use. The Act's Sections 19 (6) and 19(7) give guidelines for determining the relevant geographic market and relevant product market, respectively.

When evaluating the relevant product market, all close replacements for the product/service in question are assessed. The 'small but significant and non-transitory increase in price' (SSNIP) test is a regularly used technique for determining substitutability. This test begins by identifying the smallest conceivable relevant market and determining if the SSNIP would be lucrative in this hypothetical market or whether consumers would move to other products. In the latter situation, the market definition is broadened to include the alternative product, which accounts for 90 percent of the market. [76]Consumers change to, and the SSNIP test is repeated. As a result, the SSNIP test is a valuable framework for evaluating the demand substitutability of various competing options.

[74] Stylianos, K. and Carter, N. 2020. "The Size of the Crypto Economy: Calculating Market Shares of Cryptoassets, Exchanges and Mining Pools." Journal of Competition Law & Economics, 511-551.
[75] Act of European Commision 2002
[76] T. Schrepel, (2018). Is Antitrust Law Doomed by Blockchain? The Antitrust Paradox of Blockchain, pages 20-25

In the case of blockchain applications, there are a number of different approaches to define the relevant market. Some of the possibilities are as follows:

1. Each blockchain application as a market (since each ledger is unique): Only when there are no close replacements for the blockchain application, either in terms of other blockchain apps, non-blockchain technology, or offline equivalents, may such a market definition be appropriate. If blockchain applications are used to establish new markets that don't exist yet, this is likely to happen.

2. Blockchains with comparable applications as a single market: When there is no replacement non-blockchain applications, blockchains with similar applications can be defined as a meaningful product market. This is likely to be the case with blockchain applications that generate products or services that are new but comparable.

3. Relevant market, which includes similar blockchain and non-blockchain applications: When they are all close substitutes, the relevant product market can be defined to encompass similar blockchain applications as well as other similar digital/non-digital alternatives (if any). This is similar to considering both online and offline sales from brick-and-mortar retailers to be part of the same relevant market.

The definition of a relevant market in the case of a blockchain application is dependent on the future development of blockchain technology as well as the facts of the case (particularly the presence or absence of near replacements to the blockchain application in question). The pseudonymous nature of blockchains, as well as the capacity of the same application to span multiple locations, may make determining the relevant geographic market more difficult. Determining the geographical boundaries of the appropriate market could be difficult in circumstances when the identity of the blockchain players and their geographical location are unclear.

The pseudonymous nature of the nodes in a public, permission-less blockchain can make defining a suitable geographic market more difficult. When the identities and locations of the participating nodes are known, the relevant geographic market may be relatively easier to define. While a blockchain application may begin in one location, it can be used in a variety of locations, including international jurisdictions. In the end, the precise definition of the relevant geographic market will be determined by the facts of the case.[77]

Market power can be evaluated on a case-by-case basis using a variety of different measures. The market share of a company is one of the most important indications of market strength. When the relevant product market only consists of blockchain apps, factors such as the number of users (or active users), the number of recorded transactions, the number of blocks, the income, or a combination of these can be used to determine dominance (in addition to any other relevant factors).[78] When the relevant market includes both blockchain and non-blockchain applications, market share can be calculated using the number of users, transactions, revenues, or a combination of these factors.

[77] Op. Cit 68 pages 570-572

[78] Op. Cit. Note 5 pages 71-73

The presence or absence of entry barriers is another element taken into account when determining market power. If entrance barriers are low, market power may be constrained. In such a market, an established blockchain application with a large market share may be unable to raise its price unilaterally. In such a market, a higher price would suggest increased profitability for the incumbent, incentivizing new players to enter the market. As a result of the competition between the incumbent and new entrants, the price charged would be reduced.

A blockchain application with significant entry hurdles, on the other hand, could suggest market power. In the case of a blockchain, a new entry can potentially take the form of forking. The likelihood that a forked blockchain will also contain past data could enhance the amount of effective competition created by such an entry. Additionally, the presence (or lack) of network effects may be crucial when evaluating the dominance of blockchain applications. A phenomenon known as network effects occurs as the number of users/participants of a good/service increase. It can be difficult to use the SSNIP[79] test in technological markets where prices are zero. In such circumstances, it may be necessary to make appropriate changes to the test. [80]

Another indicator for the market power a blockchain network holds has been claimed to be the worth of the network to its users. It is common knowledge that network effects in digital markets can lead to a firm's long-term market strength. Similar network effects are anticipated to emerge in blockchain applications, particularly when the applications are set up as two-sided marketplaces.

Nonetheless the question still remains: Even if we somehow identify the market power of the network and agree that is noticeable from a competition law point of view, what is the crucial characteristic or indicator that we have dominance within the blockchain?

When a participant obtains a position of authority within a blockchain, dominance might emerge. This can be seen when entities with a dominating market position use their market power to influence the way a blockchain application works. For example, a significant existing entity may sponsor/develop a blockchain application that has the entity's support in terms of architecture, governance, and terms of participation. A mining pool with market power can unilaterally decide which blocks to verify and which should be ignored, for example, and this is an example of dominance inside a blockchain.

While such dominance and misuse have yet to be witnessed, the experience of Bitcoin mining indicates that domination is a possibility. A desktop PC was used to mine Bitcoin when it was originally introduced. However, as Bitcoin's popularity and value grew, the mining gear became more complex (ranging from a computer processing unit (CPU) to graphics processing units (GPUs), field-programmable gate array (FPGA) devices, and application specific integrated circuits (ASICs)).

In 2018, Bitmain Technologies, a Chinese company that designs ASIC chips and sells mining hardware, held over 74% of the global market. In addition, advances in mining gear made it difficult for individual miners to be successful. As a result, mining pools (a group of miners who

[79] SSNIP test seeks to identify smallest market within which a hypothetical monopolist could impose a Small Significant Non-Transitory Increase in Price. Usually defined as a price increase of 5% for at least 12 months.

[80]Op. Cit note 70 pages 30-52

pool their computing power and split the rewards based on each miner's input) and mining farms (huge mining facilities) have become increasingly popular.

So, there was less competition among miners. Instead than competing against one another, miners began to collaborate and form mining pools and farms. BTC.com, Antpool, ViaBTC, Slushpool, F2pool, and BTC.top, the world's six largest mining pools, control about two-thirds of the total hashing power[81]. Bitmain Technologies, for example, owns and manages Antpool and BTC.com, as well as being the largest investor in ViaBTC. In September 2018, these three mining pools accounted for roughly 48% of the bitcoin hash rate distribution. Because the consensus process is so important to a blockchain application, a miner's abuse of dominance inside a blockchain can have a negative impact on competition. A violation of Section 4 of the Act would be any abuse of dominance inside or by a blockchain application.

Within this spectrum we should pose and consider the following questions: Should blockchain and non-blockchain applications that provide the same service be considered part of the same relevant product market under what circumstances? In the case of permissionless blockchains, how should relevant regional markets be defined? What elements should be considered while determining blockchain dominance? What impact would the potential of a blockchain forking have on the determination of dominance? Are there any network effects in blockchain applications? From the standpoint of a blockchain application, what are the many possible entrance barriers?[82]

An example of a blockchain antitrust case is the allegation of collusion before the US District Court for the Southern District of Florida (United American Corp v Bitmain Inc) When Bitcoin Cash was scheduled for a routine protocol upgrade in November 2018, there was a disagreement between the protocol developers on the new rules, resulting in a split between the two groups into two forks: Bitcoin ABC and Bitcoin SV. The two forks fought each other for support from miners, resulting in the combined value of the forks falling below that of Bitcoin Cash before it forked.

Bitcoin ABC eventually attracted a higher number of miners and therefore preserved the name and ticker of Bitcoin cash. United American Corp has filed an antitrust lawsuit against a number of investors, mining pools, crypto exchanges, and protocol developers for allegedly conspiring to obtain maximum support for their Bitcoin ABC split over Bitcoin SV. As a result, market circumstances for mining Bitcoin currency were no longer regular, negatively impacting United American Corp's investment performance.

Konstantinos Stylianou in his article about this case makes some very interesting comments while presenting the facts of the case.[83] It refers to UnitedCorp claims that defendants, including investors, mining pools, crypto-exchanges, and protocol developers, conspired to divert hashing power to Bitcoin ABC mining while diverting market participants away from Bitcoin SV mining. According to UnitedCorp, they accomplished so by diverting mining resources from other

[82] Howell, B. 2019. "Corporate Capture of Blockchain Governance: The Next Big Antitrust Issue." April. Accessible at : https://www.aei.org/technology-and-innovation/innovation/corporate-capture-ofblockchain-governance-the-next-big-antitrust-is

[83] Stylianou, K. 2019. "What Can the First Blockchain Antitrust Case Teach Us About the Cryptoeconomy?" April 26, Accessible at: https://jolt.law.harvard.edu/digest/what-can-the-first-blockchain-antitrust-case-teach-us-about-the-crypto-economy

cryptocurrencies to Bitcoin ABC and portraying Bitcoin SV as untrustworthy. This not only impacted Bitcoin SV directly, but it also harmed Bitcoin Cash in general, contributing to the price dip, according to reports.

Was it an unreasonable restraint of trade that would have made it anticompetitive? Assuming that some kind of collusion to the effect claimed by UnitedCorp occurred (which is not self-evident, both because it would be very expensive and because stakeholder interests may have already been aligned without the need for collusion), was it an unreasonable restraint of trade that would have made it anticompetitive?

Stylianou tries to answer this question making the following analysis.[84] For one point, defendants' campaign to add hashing power to the Bitcoin Cash network appears to be capacity expansion (mining for Bitcoin ABC), which is hardly anticompetitive in the absence of any other aggravating factors. Antitrust law is usually concerned with output restrictions that lead to price rises, rather than increased output that meets more demand.

Second, both sides increased their hashing power, not only Bitcoin ABC. This is normal and expected in forking: competing forks compete for the majority of miners' support, and miners are more likely to build on the longer chain, creating a snowball effect in which the longer a forking chain becomes, the more likely it is that miners will build on it, making it even longer. As a result, mining capacity mobilization may be viewed as a mechanism for fork camps to compete, which is the polar opposite of what an anticompetitive agreement aspires for or achieves in practice.

Third, even if the essence of UnitedCorp's objection was not that miners banded together to influence the winning camp, but rather that the process was controlled to the point that the mining outcomes were not organic or natural, it is doubtful that this argument would hold up. UnitedCorp bases this argument on two factors: first, an interpretation of Bitcoin's whitepaper, which states that mining should be "decentralized" and "democratic;" and second, the fact that Bitcoin Cash developers inserted a checkpoint to the code shortly after the split to prohibit alterations.

Checkpoints are code that prohibits the protocol from reordering blocks below the checkpoint block, ensuring that even if someone gained control of the majority of mining power, the blockchain would not be changed before the checkpoint. UnitedCorp saw this as a way for Bitcoin Cash ABC developers to cement the blockchain's status as a result of the rigged mining process. These grounds may not be strong enough to support the conclusion that the trade restriction was unreasonable. To begin with, whitepapers are not legally binding, nor do they prescribe an industry standard from which participants must not diverge.

There is nothing fundamentally decentralized or democratic about cryptocurrencies, nor that this is the most efficient or welfare-maximizing market arrangement, such that interfering with these principles would violate antitrust laws. Second, while checkpoints are controversial from a governance standpoint, they are a common occurrence, and they are usually seen as a security and efficiency device.

These applications provide reasonable reasons for competition law violations, which antitrust law acknowledges as plausible defenses. To determine that checkpoints were

[84] Op. Cit. note 77

anticompetitive, the court would have to show that either these uses were inapplicable in this case, or that their anticompetitive impacts obviously outweighed their procompetitive benefits.

5.3 Abusive Behavior

As presented above it is feasible that even if in the present we cannot exactly define how and to what amount a blockchain in dominant, it is obvious that there is the possibility of a blockchain application will develop market power and become the dominant player in the relevant market. According to competition law principles, such dominance, itself, is not a problem. Any misuse thought of the dominating position, whether direct or indirect, is a violation of Section 4 of the Act and art.102 TFEU. Refusing to allow access to a permissioned blockchain is a classic example of exclusionary abuse of dominance. When might a blockchain application's limitation of access raise competition concerns? This is the important question to consider in such circumstances. For a variety of economic and technical reasons, access to blockchain applications may be limited. If the blockchain is regarded to be an essential facility and the refusal to access is unjustifiable, this limitation may cause competition difficulties. [85]

A bridge over a river that is the only means to reach consumers on the other side is a classic example of an essential facility. It may damage competition if it is held by a rival who restricts other competitors access to that bridge. Infrastructure, on the other hand, may only be regarded an essential facility if it is not easily reproducible and if it is required for organizations to operate and compete in the market. Furthermore, a competition authority can look into whether such limits encourage more technological innovation and investment in blockchain applications, which would be beneficial to competition in the long term.

Only when the anticipated anti-competitive impacts outweigh the likely pro-competitive effects are regulatory actions justified. If historical data on the ledger needs to be accessed as a crucial input for a corporate process, a blockchain application could become a necessary tool. Data can be an important facility, according to the French and German competition authorities. "Refusal to access to data can be anticompetitive if the data are a "essential facility" to the operation of the business seeking access," they write in their joint study on Competition Law and Data.

For example, a blockchain application could theoretically be created to record frequent data from IoT (Internet of things)[86] sensors put in cars. Insurance companies could use this information to calculate auto insurance premiums based on risk profiles created from historical data. If a new insurance business is refused access to this hypothetical blockchain application, it may be unable to compete effectively in the market (unless another, more expensive, mechanism for the new entrant to generate identical data exists). Thus, access to an incumbent's blockchain

[85] Hutchinson, C. S. "Potential Legal Challenges for Blockchain Technology in Competition Law." Baltic Journal of Law and Politics, April 2020

[86] Internet of Things (IoT) describes the network of physical objects—“things”—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

application may not be judged "vital" simply because the barrier to entry is high; rather, it may be so only if a new entrant has no other option to compete in the market.

Competition authorities also recognize that the refusal to access data may be held to be anti-competitive only if it can be demonstrated that the data is “truly unique and that there is no possibility for the competitor to obtain it to perform its services”. In such cases, the incumbent may be required to provide the new entrant with access to the blockchain application on fair, reasonable and non-discriminatory terms. However, while doing so, the investments made, and risks borne by the incumbent would be taken into consideration.

Furthermore, denying access, as a form of an abusive behavior, can be done in a variety of ways. Consider a scenario in which a group of rivals creates and promotes a blockchain application that is open to everyone but has a somewhat expensive membership fee. Small rivals may find it challenging to compete in the market due to the high cost. The competition study will determine if this is a case of anti-competitive cost-cutting or a normal market outcome. Thus, in such circumstances, competition evaluation focuses on determining whether the refusal to offer access (directly or indirectly) was intended to exclude a new entry (or rival) or if there were other justifiable economic or technological explanations.

To make this thought more realistic, let’s set the following example: if the entity requesting access to the blockchain application lacks the required cyber security measures, the access limitation may be justified. In the case of blockchains, denial of access might also apply to access to industry technical standards established for blockchains. The Organization for Economic Cooperation and Development (OECD) has acknowledged the "need for a technological standard for interoperability to be created by a standard establishing organization so that blockchains deployed by various enterprises can interact with one another.[87]

Some innovating ideas on blockchain technology and competition Companies adopting comparable blockchain applications may define common technical standards, similar to how corporations rely on standardization to ensure the compatibility and interoperability of their technologies.

Future standardization in this field is thought to have the potential to accelerate their growth and provide them with worldwide norms, resulting in increased interoperability and innovation. "More than percent of respondents identify a role for standards in enabling the roll out of blockchain technology," according to a survey conducted by the International Standards Organization (ISO) of governments, business, academia, and consumer organizations. Various attempts are happening around the world to establish uniform industry standards. ISO[88] established ISO/TC/307 in 2016, with the goal of standardizing blockchain and distributed ledger technologies.

On the other hand, architecture and taxonomy, use cases, security and privacy, identification, smart contracts, governance, and interoperability between blockchains are among the group's focus topics. The IEEE Standards Association (IEEE-SA), a worldwide recognized

[87] OECD, Directorate for Financial and Enterprise Affairs. 2018. Blockchain Technology and Competition Policy - Issues paper by the Secretariat. OECD

[88] The International Standards Organization (ISO) is working on a series of blockchain and DLT standards (see ISO/TC 307). While it is enormously time-consuming to develop standards, 3.5 years from now is generations in blockchain years. The ISO plans to develop a terminology standard no later than 2020

standards-setting organization, has been aggressively pursuing blockchain standardization efforts through a variety of activities in a variety of businesses and sectors, including the establishment of the world's first virtual blockchain workshop. The World Wide Web Consortium (W3C), which was instrumental in standardizing web browser functionality in the early days of the internet, now has a Blockchain Community Group that is working on a Web Ledger Protocol and has published a draft that includes "an extensible data model and syntax for expressing cryptographic ledgers, as well as a protocol for reading and writing to ledgers.

In the long run, as blockchains become more established, collaboration among blockchain participants to develop common technological standards may be necessary to assure interoperability and long-term economic benefits. This could be critical in maintaining competitiveness and fostering innovation. However, it is feasible that a dominating corporation will incorporate its proprietary technology as part of the standards, but it will then refuse to allow its competitors access to the technology. [89]

The firm's failure to give access to specified standards on fair, reasonable, and non-discriminatory terms (FRAND) terms may be regarded anti-competitive unless it is justified. A dominant position can be misused by engaging in anti-competitive behavior such as bundling, predation, discrimination, and leveraging, in addition to refusing access. In the case of blockchain applications, as with any other charge of abuse of dominance, a case-by-case approach may be used. The alleged anti-competitive activity may not always be intended at limiting market competition; it could be implemented to achieve other economic or technical goals, such as security measures.

Every case would be evaluated in line with the relevant provisions, and a suitable analysis would be conducted depending on the nature of the complaint. This is because a dominating entity's anti-competitive behavior can include unreasonable and unrelated requirements for its principal contract. For example, a dominant blockchain program may engage in anti-competitive behavior by tying access to its blockchain application to the usage of a certain digital wallet, denying its consumers the ability to use any other wallet service. In the case of such charges, a case-by-case investigation may be required, taking into account the application's core features, aim, and conduct, as well as arguments for the activity.

A dominant corporation may also take advantage of its position by engaging in predatory behavior. Predation can have two forms: OECD Competition Committee, Directorate for Financial and Enterprise Affairs (2018). The Secretariat has published a study on Blockchain Technology and Competition Policy Issues.[90] A dominant corporation may innovate or make technical modifications not for the benefit of its customers, but to destroy competitors. Predation innovation can be quickly and cheaply deployed by prohibiting access or restricting their capacity to read, submit, or validate transactions.

Another predatory method[91] that a dominant corporation may use is to lower transaction fees below cost, causing competitors to leave the market. The dominant firm will raise its price

[89] Op. Cit Note 8 p. 34 - 48

[90] Weekly FinTech Report (2018). Antitrust, Blockchain, and Standard Setting Accessible at: https://medium.com/fintech-weeklymagazine/blockchain-antitrust-and-standard-setting-3c737c03c186/blockchain-antitrust-and-standard-setting

[91] Thibault Schrepel, Predatory Innovation: The Definite Need for Legal Recognition, SMU Science and Technology Law Review, 2018 p. 23-25

and generate significant profits after the competitor(s) leave the market, allowing it to recoup the loss sustained by pricing below cost. For example, a dominant blockchain may decrease its transaction price dramatically to drive a competitor out of the market, then raise the fee once the competitor has left. Predatory behavior would be evaluated in accordance with the Act's applicable provisions. The Act defines predatory pricing as "*the selling of products or provision of services at a price that is below the cost of production of the goods or provision of services, as defined by rules, with the intent to reduce competition or eliminate competitors*".

This is less likely in a blockchain where transactions are validated by PoW consensus because miners compete for the transaction fee by verifying transactions (or token currency). Allegations of discriminatory pricing would be investigated under the Act's applicable sections. Leveraging by exploiting its market power in one market to enter/strengthen its position in another, a dominating organization might have a negative impact on competition. Leveraging can be done in a variety of ways. For example, a dominating blockchain application may raise transaction fees and use the additional income to provide wallet services at a reduced cost, thus forcing competitors out of the market.[92]

While evaluating charges of such conduct, a case-by-case analysis based on the features and behavior of the blockchain application may be conducted. Both permissioned and permissionless blockchains can be used to abuse supremacy. In the case of public permission-less blockchains, however, such behavior may be conceivable only if the governance rules are set up to allow it. This could necessitate collaboration and agreement among the nodes. The capacity to engage in such behavior in a blockchain application is thus determined by the governance rules, which include how easy it is to modify the governance. In comparison to a permission-less public blockchain, changes in governance may be made far more readily in a permissioned consortium blockchain.

As mentioned and analyzed above, to some extent, all information and transactions recorded on public blockchains are visible to everyone. Transactions on private blockchains are only visible to their users if they are built that way. As a result, the number has increased. On public blockchains, the prevalence of anti-competitive practices may be lower than on private blockchains. Because public channel chains provide greater value in technology markets, user-to-user transparency. So, given that transactions can be watched by everyone, it is to be expected.

The intrinsic transparency of blockchain users tends to hinder the implementation of anti-competitive practices, thus reducing overall anti-competitive conduct. Nonetheless, caution is essential, as unilateral activities would not completely vanish as a result of the blockchain's implementation, also known as the "opacity effect". All transactions on the blockchain are encrypted, and anonymity protects the identity of blockchain users. Although the transaction is visible, the substance and purpose of the transaction are not. Outsiders are unaware of the interaction between users, making it opaquer. This is even more prominent in private blockchains, where the content of transactions is kept hidden. Someone could claim that outsiders are kept in the dark about the blockchain.

Christophe Samuel Hutchinson[93] to illustrate which unilateral anti-competitive practices might be implemented on a blockchain, presents an assumption of the hypothetical situation of the

[92] Op. Cit Note 30 pages 50
[93] Op. Cit Note 79

firm Y operating in a digital market. Y decides to develop a private blockchain as part of its diversification strategy. The blockchain is designed so that Y can choose the users who may access it, which operations users can perform, as well as the governance protocol. It is also able to update these settings, should it choose to do so, any time in the future. Y uses its blockchain to develop BlockJobs, a professional social network that allows users to find job adds and apply for new jobs. The blockchain records information through a smart contract throughout the recruitment stage. Following its application success, Y's competitors are also utilizing its platform to attain new talent, which forces Y to develop a strategy to minimize competition. Using this case, Hutchinson covers a wide spectrum of anti-competitive practices entities could implement to gain unfair competitive advantages. We will use this case to supplement the range of anti-competitive practices analyzed below.

5.4 Exclusionary Abuse Through the Use of Blockchain Platforms

Refusal to deal, tie-in sales, predatory pricing, margin squeeze or exclusive dealing, and rebates are examples of exclusionary abusive practices. When a monopolist refuses to deal with a competitor, Article 102 TFEU, which forbids the abuse of dominant position, is activated. Although a company's responsibility to deal with its competitors is often absent, the European Court of Justice has found antitrust liability where a monopolist refuses to sell a product to a competitor that it makes available to others.

Outside of blockchains, refusal to deal is a widespread practice, but it should not be a big issue in blockchains, especially public blockchains. Although a public blockchain is built to allow public access, a refusal to grant access to it would have to be implemented in its governance design. It is not possible to select users in a planned or exclusive manner. As a result, the refusal to trade can only be implemented by changing the access rules. Exclusionary techniques are thus incompatible with the inherent nature of public blockchains, and blockchains that use them will no longer be regarded "public." The refusal to provide general access, on the other hand, is a key feature of private blockchains.

Depending on the governance choices, the gatekeeping mechanism within such permissioned blockchains may take various forms, such as hindering access to information for competitors, and validating transactions, among others. For example, a "refusal to use the blockchain" might be used to "exclude maverick enterprises or new entrants," as well as "exclude or boost the expenses of rivals outside the consortium."[94]

We will pretend that a blockchain exists among European banks for interbank payments to show a situation of refusal to deal (not allowing a business to join a blockchain community). There may be a genuine alternative - the old approach – of clearing interbank payments, but it is slow and expensive in contrast. If a new bank wants to start doing business in Europe, being a member of the blockchain may be required if it wants to compete. If the new bank is denied access or membership for nonobjective reasons or on a nonobjective and reasonable cost basis, this may be considered an abuse under article 102 TFUE. Exclusionary attempts by gatekeepers risk violating

[94] Innovation & Technology Business School. 2020. "e-zigurat." e-zigurat.com. Accessible at https://www.ezigurat.com/innovation-school/blog/public-vs-private-blockchain-whats-the-difference/

Art. 102 TFEU if permissioned blockchain gains the character of vital infrastructure and refusal to allow access to it is not objectively justified.

5.4.1 Tying/bundling[95]

Tying refers to an entity selling goods and services with a condition to seek further sales and commitments from its counterparts. It can also mean subjecting a contract to the acceptance of extra duties and commitments that are completely different to the contract's original subject. In public blockchains, tying is unlikely to occur. This form of blockchain is, in fact, fully available and functional. As a result, it is unlikely to be sent to another product or blockchain.

Private blockchains, on the other hand, may have a vested incentive in enforcing tying or other similar behaviors if they are built by for-profit organizations. Bundling effects can develop when an entity combines the use of a blockchain platform with services that are provided outside of the blockchain and on which the company has a dominant position. As a result, tying is more likely to occur on private blockchains.

5.4.2 Squeezed Margins as an Abusive Behavior

An abusive behavior through squeezed margins can occur when a dominant entity is able to set prices very high so that its competitors are not able to compete fairly over the long-term. However, since public blockchains are horizontal by nature, the likelihood for public blockchains to be subjected to a margin squeeze is low. Private blockchains, on the other hand, are a different story. Such an abusive practice has not been widely reported yet, but it still has to be monitored closely as this might change as blockchain platforms grow in the future.

5.4.3 Exclusive Dealings

Dealings that are exclusive are also prohibited by article 102 TFEU. In such a case, a market participant with monopolistic power might require that in order for its customers to utilize its blockchain to complete transactions they must stop using the competitor's blockchain. Yet, since using more than one blockchain for a transaction requires effort and time, users are disincentivized to use multiple public blockchains. Yet, this is not always the case for private blockchains. [96]

Entities developing private blockchains strive to attract and retain users by promising a range of data that would only be available on their platform. In this case, by providing a proprietary range of data an entity might want to ensure that its users are only utilizing its platform, which

[95] Op. Cit. Schrepel note 91 p. 27

[96] Op. Cit note 79 pages 61-63

also helps in enhancing its reputation. In the case of BlockJobs, for instance, Y might wish to be the only firm that lists certain types of job opportunities. To that purpose, BlockJobs may wish to impose an exclusive deal at the blockchain's entrance point.[97]

5.4.4 Rebates[98]

Rebates can also be used as an anti-competitive strategy, indirectly rewarding users that prefer the dominant entity’s platform. Yet, since in public blockchain, all transaction information is publicly available and easily accessible, the likelihood for such practices to occur is limited, as it may harm the platform’s reputation in case these are conducted in an unfair and unjustifiable manner. In private blockchains, however, the likelihood for such practices to be implemented rises significantly.

5.5 Exploitative Abuses

Exploitative abuses can occur when certain customers and/or suppliers are treated unfairly. In regards to blockchain, exploitative abuses can occur when blockchain network participants require to be treated preferentially in order to provide their services. Exploitative abuse, though, has not been a big issue yet in blockchains. Experts state that the innovative environment of blockchain will minimize the need for such abuses, though this does not mean that such abuses will not happen.[99]

5.6 Discriminatory Abuses[100]

A discriminatory abuse can occur when entities engage certain parties advantageously, thus creating a competitive advantage for those parties as well as a competitive disadvantage for everyone else. The most usual type of discriminatory abuse is price discrimination. As this means that certain customers are favored over everyone else, price discrimination usually happens when the same product is sold to various customers at a different price. Due to the fact that transaction information in a blockchain can be easily observed and verified, however, it is unlikely that price discrimination will be a significant issue.

Yet, discriminatory abuses are not limited to pricing, and in a blockchain in particular it is more likely for a discriminatory abuse to occur in cases where certain users are favored to join a blockchain network more easily than others. In this case, a very high entry price would favor certain users to become and remain members of a particular blockchain network. For this reason, discriminatory abuses are less likely to occur in a public blockchain, where transaction information is much more easily verified.

[97] Op. Cit Note 79

[98] Bill Batchelor and Sophia Real, Baker McKenzie, A practical approach to rebates, Thomson Reuters , 17-Jan-2018 European Union, page 2/12

[99] Op, Cit Note 79

[100] Op. Cit note 5 pages 89-94

6. PART C – CONCLUSIONS AND SOME FURTHER THOUGHTS

6.1 The Root of the Problem: The Essential Concepts of Competition Law

The above analysis highlights that there are a lot of arising issues, discussions and opinions about the interaction between blockchain technology and competition law. The innovative technical characteristics of blockchain technology as well as its way of functioning does not seem to be in line with the logic on which competition law is built. This results in serious practical problems when it comes to the application of competition rules in Blockchain platforms.

Competition law uses terms like ‘’firm’’, ‘’company’’, ‘’relevant market’’ and ‘’dominant position’’. These terms acquire meaning within the context of the need that created them, which is no other than the need to regulate merger and acquisition process and the control of the market by oligopolists or monopolists. The question that raises, the one that we are trying to answer in this dissertation is what could possibly happen with the application of competition law in a continuously changing and growing environment where these structures appear more and more less and they are instead giving their place in anonymous communities? How we apply competition law in an environment where we do not have a central unit but many decentralized networks?

As already exposed above with respect to the main legislative framework of Competition Law, competitive authorities are trying to limit -or even prohibit- partnerships between undertakings that they might be harmful to consumers’ welfare or partnerships that limit or disturb the well-settled functioning of the competitive procedure. At the same time, these rules define the guidelines as to what is permitted and what is not when it comes to vertical acquisitions, analyze proposed acquisitions and block any action that would lead to concentration of power and maybe abuse of this power in the market with possibility of harm the consumers’ welfare. In all of these cases though, the prerequisite is the existence of an undertaking (or a consortium of undertakings). This undertaking then would be questioned by the Competition Authorities and from the questionings’ outcome fines would be imposed or prosecution would take place.

The point is that blockchain technology introduces a new system of decentralized management and function. At the same time, totally eliminates the need of existence of an undertaking having the role of a middleman and handling the transactions taking place in a digital platform. In fact, this is what is considered more valuable and makes public blockchains so promising for the future of the economy and transactions: its decentralized character. The decentralization in blockchains not only abolishes the need of a middleman, reduces transactions and bargaining costs and separates its existence from a central firm, but most important establishes that this platform is autonomous and independent. It does not require any type of support from other undertakings to function.

At the present time, we cannot conclude that any of the currently powerful blockchain platforms have acquired such power that it is a clear threat under the pretext of competition law. Of course, the whole development of these platforms as well as their market power is constantly and ever-changing to the extent that the data are different from month to month. Nevertheless, some platforms have already established their presence, reputation and relatively their market power and someone could foresee that these platforms are very likely in the future to obtain more power and play a significant role to the conformation of pricing and other anti-competitive behaviors.

If people necessary for the operation of blockchain platform, such as the miners in a blockchain platform similar to Bitcoin, take advantage of their control/impact on the inflow in order to carve out competition in this decentralized market, it would be extremely difficult for the competition authorities to take any action, due to the fact the subjects who tried to cause/ or caused the violation of Competition rules could barely be identified. Then, even if we are able to identify these people, we could not make sure that we could define them as ‘’economic entity’’, ‘’firm’’ or ‘’undertaking’’- characterization which is essential when it comes to application of competition legal rules.

This happens due to the fact that according to European Competition Law reliable can only be entities engaged in economic activity. This can have serious exclusion of responsibility effects. For example, the people using cryptocurrencies only for private purposes, i.e. mainly to buy goods and services for personal use could not be found liable for any of their actions even if these would resemble to a violation of antitrust law, since the characterization of ‘’entity engaged in economic activity’’ cannot be attributed to them.

In some of these cases it is not clear what the level of accountability of the co-participants in a blockchain network is, such as the validators of new blocks, when they actually act without any profit – driven motivation. Actually, some of them might act on the basis of idealistic incentives or doing this as a hobby. Nonetheless, in case of certain cryptocurrencies where validators clearly have speculative incentives, plans for maximization of the profit as well as collaborations with investors and even some time employers under their supervision, they would more probably be found accountable and they would not be able to counterargue that they are not engaged in economic activities.

The same issue arises also when it comes to the users of the cryptocurrencies, while additionally in this case we also face the problem of defining the relevant jurisdiction from geographic point of view. But still, in case we actually make it to define the jurisdiction the question is who is responsible and how can we track this person or group of persons when all the participants in a blockchain network are anonymous and all the digital data are registered and saved everywhere across the network and at the same time?

The answer to who is in charge has to be given clearly when we focus on a network whose one of the main characteristics is anonymity. Even if we fully analyze the network and we are able to have relatively valid information about the nodes’ identity, it still remains quite complicated to collect sufficient evidence showing that the nodes are under common control especially when it comes to nodes operating and trading in different platforms.

Also, at this point we need to underline the issue that arises from the other characteristic of blockchain technology, this of cryptography. The level of difficulty as to accurately define the information registered in a blockchain ledger, due their encryption, especially in the case of cryptographic keys being destroyed is huge. Additionally, in case of closed blockchain platforms the registered data are not necessarily unchangeable and nodes participants could theoretically conspire and reform falsely the ledger before they are investigated by the Competition Authorities.

6.2 Private and Public Blockchains

Having said that, someone could wonder what we see as the key exclusionary concerns that may be posed by blockchain technology when it comes to the coordination with Competition Law?

One of the conclusions that someone could easily draw is that it is very important to distinguish between public and private blockchains. As far as public blockchain is concerned, the likelihood of anti-competitive practices being committed as of today is quite low. This happens for three reasons:

The first reason, which is highly connected with the structure of competition law and its essential concepts, is that public blockchains do not have a proper governance in the sense that this concept is used to be understandable, like having a pilot to a plane. So, because of that, it is very hard within public blockchain to actually choose a strategy in general, but also a unilateral strategy and then implement it.

The second reason is their characteristic of being unmodified. In fact, as mentioned above, it is quite difficult to modify the way a public blockchain functions. Thus, in case of planning any anti-competitive agreement or act, it will be requested from the subjects willing to commit this act to find a way to implement the possibility of later of committing anti-competitive practices from start, from the day one of the blockchain 's creation, something that in realistic terms is very unlikely to happen.

The third reason is the so called ''visible effects''. Everything happening in public blockchain is public and seen by all participants in the blockchain. This reduces the incentives to plan and act towards anti-competitive practices, since if this anti-competitive behavior take place will be seen by all participants in the network. Nonetheless, most of the public blockchain platforms are now working on new governance systems. This increases the possibility of adopting the system in such a way that could actually favorite much more the existence of a pilot on the public blockchain, as mentioned above.

With regards to private blockchains the situation is quite different from public blockchains. There are two reasons that this is happening: Firstly, private blockchains, contrary to public ones, they actually do have a governance, they do have a way to unilateral practices and they can also modify the way they function really easily without the need of approval from the blockchain's participants. In other worlds, any time there might be a decision and coordination towards anti-competitive behaviors.

Secondly, in private blockchains the element of ''visible effect'' is absent -unless of course private blockchain is designed this way. The rule though in private blockchains is that the data registered are not seen by all and usually the users that can access and see the transactions are chosen and this obviously raises the possibility of appearance of anticompetitive behaviors.

Due to its decentralized nature, the blockchain is able to prevent monopolies, reducing the likelihood of a centralized entity forcing other entities to comply with its requirements and strategies. A blockchain by itself does not facilitate dominant position or any other type of abuses. As such, interested parties should not be concerned about being abused or about other parties' efforts to hinder competition. Currently, the blockchain is still in its first stages of development with most of the focus being on creating new opportunities, rather than taking advantage of the technology to unjustly solidify market position and gain unfair advantages.

This dissertation 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 blockchains, since antitrust law does not provide complete answers to three questions: how anti-competitive practices committed on public "permission-less" blockchains can 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?

The problem is while the architect of an anti-competitive practice on blockchain can sometimes be identified, the effectiveness of sanctions and remedies may be hindered by the immutability of the blockchain. 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 a rival may be excluded based on business and competitive aspects, following the recommendations of antitrust best practices would help assess and reduce antitrust risk. Membership criteria should be appropriately explained and justified, having in mind the requirements in ensuring fair and equitable competition. Another challenge to competition with regard to the use of blockchain as exposed above, 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 Department of Justice, the Federal Trade Commission or the European Commission, of vertically designed rules and concepts of antitrust law to a technology built around the desire for decentralization.

There is the need to find new ways of decentralizing antitrust law and antitrust authorities should be updated through new governance models that support the use of blockchain. International legislation, and especially European legislation, must recognize and focus on addressing the relationships and market conditions that new technological innovations such as the blockchain create. This would help reinforce the regulations to protect the users of innovative technological applications, and minimize abusive, anti-competitive conduct. Any updates and revisions must take into considerations the different conditions in regards to how likely each member in the EU is to utilize blockchain applications, and whether and how local law, in addition to EU law, covers such aspects.

Overall, the blockchain technology has already started significantly impacting almost every market across the EU economies. Despite the grey areas with regard to competition law, general antitrust concerns on blockchain are the same as in existing traditional markets and technologies. As a result, governments and competition authorities will need to keep applying existing theories of damage and focusing on rivalry, substitutability, and management of competing products.

We recommend that government authorities should focus on the development of permissioned blockchains, as well as investigate the design protocols of such blockchains and consider providing advice and asking to participate in the development of such blockchains. As a network node, anyone can participate. The risk that blockchains pose should be the second point of concern, as a result of successful foreclosure or purchase by dominant network participants. However, as with many other innovative products, there are certain drawbacks. Regulatory agencies should begin by conducting exploratory market studies in order to grasp the blockchain technology's nature as well as the threats and opportunities it presents.

Furthermore, in cases where a blockchain is regarded as dominant, it is challenging to indicate the participants that benefit from the dominant position. As there exist multiple ways to characterize a dominant position, it is also challenging to successfully attribute liability to the participants that benefit from a dominant position and their actions. As such, it is crucial to carefully define how a dominant position may be achieved in a blockchain, as this would provide the basis for attributing liability in regards to any actions taken across the network.

In general, the blockchain technology can not be characterized as pro or anti-competitive in nature. Legal and economic experts indicate that it is very challenging for a blockchain to achieve a dominant position. There are, however, certain cases where abuse of dominant position can be indicated where dominant participants might directly or indirectly refuse to grant access to a particular blockchain network to interested new members by making entry requirements unreasonable and nearly impossible to comply with (very high entry costs, time required to comply with requirements and make transactions).

Blockchain as a Tool of Enforcement of Competition Law

In the second and third part of this dissertation we exposed what has been written and questioned from legal experts and economists about the issues that have been raised when it comes to the investigation of the competition authorities and the application of legal rules mainly due to the special characteristics of the blockchain technology and the foundation and essential concepts in which competition policy has been built. In this section of the project, we will try to demonstrate and propose a different way of interaction between blockchain and competition. In fact, we will try to give the answer to this question: How can a blockchain facilitate the implementation of competition law?

One of the key features of a blockchain is that it is distributed, immutable and a secure ledger. This attribute may assist competition authorities towards enforcement of the competition law. A major challenge usually faced by competition authorities while investigating allegations of anti-competitive conduct is the paucity of information and data to provide the necessary evidence. Often the data procured from the parties to conduct an investigation is not verifiable from a third-party source.

However, in blockchain applications, the necessary information could be obtained by viewing the ledger of the blockchain application (which have been verified and cannot be altered). For instance, if there is an allegation that competing firms using a blockchain application have cartelized, then by accessing the transaction information on the blockchain, it is possible to analyze the data to determine whether there is economic evidence of collusion or not. Similarly, data from a blockchain application may also facilitate with an assessment of how a proposed combination of firms (merger, acquisition, or joint venture) is likely to influence the competition.

Nevertheless, the ability to analyze data from a blockchain comes with certain challenges. In the case of public blockchains, some data could be encrypted and pseudonymous, while in the case of permissioned consortium blockchains, there exists a possibility to access the data on the blockchain.

Further, under the leniency programs, in the case of blockchains, the firm making the leniency application may be able to use the blockchain application itself to collect and provide extensive information to assist the competition authorities in their investigation. For instance, if a cartel among the firms in a blockchain application exists that shares competition-sensitive information amongst each other, one of the cartel members can file for leniency and support the competition authorities by providing the data available from the blockchain application.

Finally, blockchains may also improve competition law enforcement through the use of smart contracts, specifically, to ensure that a firm complies with the commitments it has proposed and which the competition authority has accepted. A smart contract can be introduced within the blockchain in which the firm participates to self-enforce adherence to the conditions of the commitment. For instance, if a firm commits that it will not raise its price by more than 10% in a year to ensure compliance, the competition authority can introduce a smart contract that permits the sale by the entity only if the price increase is not more than 10% of the price charged in the previous year. This might significantly save cost and effort that would have otherwise been incurred in monitoring the compliance to the commitment.

In conclusion, we could support that the competition authorities are not the only ones who are challenged by blockchain technology. It also gives them numerous opportunities to help them with their task. For example, if DLT is utilized to submit leniency applications, cartel enforcement may become more successful, but also to deal with the massive amount of evidence that is typically collected in a competition law case. Access to the file will also be easier to regulate, resulting in more effective security A data stream may also be accessible to competition authorities and courts.

All relevant transactions are kept on the blockchain. This could be useful knowledge in the future in order to offer evidence of a violation of competition law, but also in the context of legal activities a claim for damages. The availability of this information would also make market monitoring easier, and allow for the early identification of cartels and other anticompetitive practices by competition authorities' activity.

8. Bibliography

Androtsopoulou, O.S 2019 ‘’Blockchain Technology : Treats & possibilities , Athens

Albertorio, A. 2020. "Simply Explained: Why is Proof of Work Required in Bitcoin?" January 7.

Artzt, M., and Richter, T. 2020. *Handbook of Blockchain Law: A Guide to Understanding and Resolving the Legal Challenges of Blockchain Technology* . Kluwer Law International BV.

Artzt, M., and Richter, T. 2020. *Handbook of Blockchain Law: A Guide to Understanding and Resolving the Legal Challenges of Blockchain Technology* . "Blockchain and Antitrust."

Breu, S. U. 2017. "Blockchain and cryptocurrencies challenges Anti Trust and Competition Law." *SSRN Electronic Journal*, January: 3-4.

Capobianco, A., and Pike, C. 2020. *Antitrust and the trust machine.* OECD Blockchain Policy Series. https://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf.

Competition Comitee of India. 2021. "Discussion paper on Blockchain Technology and Competittion."

Conway, L. 2021. "Blockchain Explained." *Investopedia.* June 1. https://www.investopedia.com/terms/b/blockchain.asp#decentralization.

Elig Gurkaynak. 2020. Horizontal Agreements. https://www.mondaq.com/advicecentre/content/1548/Horizontal-Agreements.

Euromoney Institutional Investor, PLC. 2020. "Euromoney Expertise: What is Blockchain." https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain.

European Comission. 2002. "The Competition Act ."

European Commission. 2008. "Consolidated version of the Treaty on the Functioning of the European Union - PART THREE: UNION POLICIES AND INTERNAL ACTIONS - TITLE VII: COMMON RULES ON COMPETITION, TAXATION AND APPROXIMATION OF LAWS - Chapter 1: Rules on competition - Section 1: Rules." *Official Journal 105*, 05 9: 89. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12008E102.

European Commision. 2020. *Guidelines on the application of Article 101(3) TFEU (formerly Article 81(3) TEC).* European Comission.

European Commission. 2020. "Shaping Europe's Digital Future." *EC EUROPA CITE.* https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf. Publications Office of the European Union.

European Comission. 2021. "Revision of the two Block Exemption Regulations for horizontal cooperation."

Howell, B. 2019. "Corporate Capture of Blockchain Governance: The Next Big Antitrust Issue." April. https://www.aei.org/technology-and-innovation/innovation/corporate-capture-of-blockchain-governance-the-next-big-antitrust-issue/

Huilet, M. 2020. *Bitcoin Will Follow Ethereum And Move to Proof-of-Stake.* April 4. https://cointelegraph.com/news/bitcoin-will-follow-ethereum-and-move-to-proof-of-stake-says-bitcoin-suisse-founder.

Hutchinson, C. S.. 2020. "Potential Legal Challenges for Blockchain Technology in Competition Law." *Baltic Journal of Law and Politics*, April.

Innovation & Technology Business School. 2020. "e-zigurat." *e-zigurat.com.* https://www.e-zigurat.com/innovation-school/blog/public-vs-private-blockchain-whats-the-difference/.

Jakobsson, M., and Juels, A. 1999. *Proofs of Work and Bread Pudding Protocols.* Deventer: Kluwer, B.V.

Kumar, K. 2021. *Proof Of Work In Blockchain | What Is Proof Of Work | Proof Of Work Explained | Simplilearn.* Directed by Krishna Kumar.

Lianos, I. 2018. *Blockchain and Competition.* London: Centre for Law, Economics and Society (CLES).

Massessi, D. 2018. "Public Vs Private Blockchain in a Nutshell." https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f.

Organisation for Economic Co-operation and Development (OECD). "Data and Competition."

OECD Secretariat. 2018. "Blockchain Technology and Competition Policy - Issues paper ." *Blockchain and Competition.* Organisation for Economic Co-operation and Development. 2.

OECD, Directorate for Financial and Enterprise Affairs. 2018. *Blockchain Technology and Competition Policy - Issues paper by the Secretariat.* OECD.

Official Journal of the European Communities (*OJ)* . 1997. C372 (European Court of Justice, 12 9).

Schrepel, T. 2018. "Is Antitrust Law Doomed by Blockchain ? The antitrust Paradox."

Schrepel, T.. 2020. *LIBRA: A CONCENTRATE OF "BLOCKCHAIN AND ANTITRUST".* MICHIGAN LAW REVIEW online.

Stylianou, K. 2019. "What Can the First Blockchain Antitrust Case Teach Us About the Crypto-economy?" April 26.

Stylianou, K. and Carter, N. 2020. "The Size of the Crypto Economy: Calculating Market Shares of Cryptoassets, Exchanges and Mining Pools." *Journal of Competition Law & Economics,* 511-551.

Tagara, M., and Shoning, F. 2018. "Blockchain: Lessons learnt from the net Neutrality Debate and Competition Law realated aspects." *Concurrences N°3-2018 I Legal practices*, 3.

DECLARATION OF NON-INFRINGEMENT OF COPYRIGHT

I declare responsibly that the thesis I am submitting does not contain any evidence of copyright infringement in accordance with the following terms which I have read and accept:

1. The thesis must be the work of the candidate who submits it.

2. Copying or paraphrasing a third party's work is an infringement of an intellectual property right and constitutes a serious offence, equivalent in severity to copying during the examination. This offence includes both infringing the intellectual property rights of another diploma candidate and copying from published sources such as books, papers or scientific articles. Plagiarised material may come from any source. Copying or using material from the Internet or an electronic encyclopaedia has the same adverse legal consequences as using material from a printed source or database.

3. The use of extracts from the work of third parties is acceptable provided that the source of the extract is acknowledged. In the case of verbatim quotations from the work of another, the use of quotation marks or a footnote is necessary so that the source of the quotation is acknowledged.

4. Paraphrasing text is an infringement of intellectual property rights.

5. The sources of the extracts used should be fully listed in a bibliography table at the end of the thesis.

6. Infringement of intellectual property rights is subject to sanctions. In determining the appropriate sanctions, the relevant School bodies will take into account factors such as the scope and size of the part of the thesis that constitutes an infringement of intellectual property rights. Sanctions will be imposed, following the opinion of the three-member examination committee by decision of the Faculty Assembly, and may consist of the zeroing of the thesis (with or without the possibility of resubmission), removal from the graduate student registers, and the imposition of disciplinary sanctions, such as the suspension of the student status of the diploma candidate.

In addition, I give my consent for an electronic copy of my thesis to be subjected to an electronic check to detect any evidence of copyright infringement.

Date
Candidate’s Signature

14.11.2021