CAN ANTITRUST TRUST BLOCKCHAIN?

(Algorithmic Antitrust, Springer, 2021, Forthcoming)

Giovanna Massarotto[1]

Abstract: Governments must anticipate today's fast moving technologies to be effective. Blockchain potentially is the ideal tool to assist antitrust in enforcing regulation and fully exploiting its core principles—competition and consumer welfare. Blockchain offers antitrust an enormous opportunity and as any powerful tool it also has the capacity to harm as well as benefit if abused and left totally uncontrolled. Blockchain is not immune from the economic principle of *trust*. This chapter explores the delicate balance between regulation of and for blockchain.

1. Introduction

Blockchain should bring a sense of wonder to people in the field of antitrust. At least, I found myself fairly curious about this technology, as blockchain can give the edge antitrust needs. Blockchain can decentralize today's centralized platforms governed by the so-called *Big-Tech*. On the other hand, *smart contracts* that run in an antitrust blockchain, can auto-enforce most of antitrust remedies and rules. In other words, as explored throughout the chapter, blockchain technologies can be what antitrust needs to tackle its present challenges: *Big Tech* and data-driven markets. (Massarotto, 2019a)

However, blockchain technology is far from being perfect. Permissioned and closed blockchains can, for example, create the perfect conditions for competitors to engage in cartels; smart contracts, on the other hand, can automatize the punishment for any cartel's deviation. Although blockchain is decentralized by designed, today this technology is in practice in the hands of few corporations—antitrust can be crucial in restoring blockchain's decentralization (Massarotto, 2019b; Massarotto 2020a)

Having provided a toolkit to navigate into the blockchain ecosystem of Distributed Ledger Technologies (DLT), Section 3 investigates the relation between competition and blockchain. *Is blockchain the real game changer for today's centralized digital markets?* (Massarotto, G. (2020d) Section 3 explores the exploitation of DLT as a tool to enforce antitrust principles more efficiently in today's tech-digital economy. In particular, it will be analyzed if blockchain and DLT in general can be considered as a revolutionary progress also in the context of antitrust (Massarotto, 2019a; Massarotto 2020a).

Section 4 bears the question as to whether blockchain raises antitrust concerns and how to deal with them. Technologies are not the driver of anticompetitive conduct, but forms of government surveillance, such as antitrust, are fundamental for keeping people's trust in new advanced technologies. (Massarotto, 2019b; Werbach, 2018).

2. Distributed Ledger Technologies Toolkit

Blockchain is a technology that emerged in 2008 with the introduction of bitcoin, in a time where the bank system was facing one of the worst crises ever (Massarotto, 2020b). To recognize the

[1] Research Associate UCL CBT, Adjunct Professor University of Iowa (USA).

potentialities and possible antitrust concerns behind this technology, it is necessary to analyze its origin, characteristics, applications, and its most recent developments.

Blockchain, along with cryptocurrencies and smart contracts, is part of the so-called *Distributed Ledger Technologies* (DLT) (Tasca & Tessone, 2019) analyzed here. Section 2 starts with an overview of blockchain origin and DLT, focusing on blockchain, blockchain tokens and smart contracts. It proceeds with the investigation of the most recent developments and applications of DLT and how this technology has the potential to revolutionize markets yet again.

2.1. Blockchain origin

There is nothing more intriguing than studying the origin of blockchain, which dates back to the 1990s and the rise of the *Cryptoanarchy* movement (Wright & De Filippi, 2018). The main idea that drives the Cryptoanarchy movement is that computer protocols can deal with policies, such as privacy, security and economic policies, much better than governments (May, 1994). In 1988, Timothy C. May, who is considered the father of the Cryptoanarchy movement, wrote the "Crypto Anarchist Manifesto" (May, 1988). In his Manifesto, May explains how cryptography hardcoded into computer protocols (*cryptographic protocols*) can completely reshape "the nature of government regulation, the ability to tax and control economic interactions, [and] the ability to keep information secret [protecting privacy]" (May, 1988) without any government interventions. The anarchy is here conceptualized not as total chaos or disorder, but rather as the absence of a central government (May, 1994). Notably, the government creates and enforces rules to preserve justice and people's freedom; computer technologies can create self-enforcing rules without involving the government. (Ou, 2017)

A key figure in the cryptoanarchy movement is David Chaum who created e-cash, the predecessor of bitcoin. E-cash was presented in 1983 as anonymous electronic money that would enable people to spent digital money without the need of having a bank account. Privacy and security would have been protected by means of public key cryptography, which is a cryptographic system based on pairs of keys: a private and public key. Data is encrypted with the public key and security is preserved maintaining only the private key; the public key can be openly shared because only the owner of the private key can decrypt data encrypted with the public key.

Although e-cash was a promising project, we need to wait for the bank crisis of 2008 to see the idea of using anonymous electronic money to expand. In addition to being anonymous and digital, bitcoin is decentralized and does not rely on the bank system. Bitcoin uses a peer-to-peer network called *blockchain network* as platform for bitcoin transactions, ensuring anonymity and security through the same public key cryptography adopted in e-cash. Blockchain is not the first peer-to-peer network. Notable examples are BitTorrent and Napster (Bashir, 2017), but in addition to sharing data blockchain peer-to-peer network stores data.

2.2. Blockchains

2.2.1. Bitcoin Blockchain

In November 2008, an anonymous person (or group of people) under the name of Satoshi Nakamoto introduced a distributed system for electronic transactions, which included Bitcoin and blockchain. (Nakamoto, 2008) Blockchain seems to be what the cryptoanarchy movement dreamt about. Blockchain is built on the idea of a fully decentralized peer-to-peer network, where no one controls the blockchain. It is a set of rules enshrined in a computer protocol that governs the blockchain network. If everybody follows the rules, everybody wins and the blockchain functions properly.

The bitcoin blockchain protocol sets a consensus mechanism known as *Proof of Work* (PoW) to transfer bitcoins. Instead of having banks that validate a transaction, the PoW requires participants in the blockchain network to resolve a computational problem. The first participant that finds the solution broadcasts it to the blockchain network. Only when the majority of participants agree on the solution is the transaction validated and stored in a block that becomes part of the chain. Thanks to the public key cryptography (PKC) the parties of the transaction remain unknown. The public key, which is broadcasted to the network, is never attached to the real name of the owner. The identity of Satoshi Nakamoto is still unknown, showing the validity of cryptography in protecting users' identity and privacy. Many people in the field suspect that the same cryptoanarchy movement is behind the creation of bitcoin and blockchain.

Blockchain safety is another key component of this technology. Blockchain safety is guaranteed by using a vast number of computers called nodes. A cyber-attack in a blockchain would require striking almost all copies of the ledger simultaneously (hence the blokchain network), and would cost billions of dollars. (Massarotto, 2019b) In addition, as Nakamoto (2008) observed, "[t]o modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes" (p. 3).

Introduced as technology to exchange bitcoins, blockchain is now adopted in a variety of industries, from cryptocurrency to social applications and consumer goods (Massarotto, 2020a; UCL CBT, 2019). Walmart, for example, adopted blockchain in its supply chain to track goods, which enabled Walmart to do what usually was performed in seven days in 2.2 seconds (UCL CBT Supply Chain Report, 2019; Hyperledger).

In summary, blockchain, can be used to record and store not only financial transactions, but "virtually everything of value," (Tapscott D. & Tapscott A., 2016) bypassing third intermediaries, which in the case of bitcoins means banks. DLT eco-system now includes a plethora of different blockchains (e.g. private and permissioned blockchains) and emerging technologies, including smart contracts and blockchain tokens explored in the following.

2.2.2. Public, Private and Permissioned Blockchains

Bitcoin blockchain is the very first blockchain, introduced in 2008. But over the years, software developers have built up a variety of different types of blockchain: the main distinction is between public and private blockchains. Bitcoin blockchain is a public blockchain. This means that it is open and free to anybody wants to participate in the blockchain network. Private blockchains, instead, are closed networks and you need to be invited to participate in the chain. Both public and private blockchains can define different levels of permission for participants creating a kind of hierarchical authority (Tasca & Tessone, 2019). For example, all participants can have read access, while only a pre-select set of nodes has the permission to write and manage the blockchain (European Commission, 2019).

Forms of private permissioned blockchains especially attract banks, government departments and any enterprises interested in implementing blockchain as a kind of internal infrastructure similar to an intranet, but that function as decentralized database. It is common to hear that "public blockchains are to the internet as private blockchains are to the intranet," (Eichholz, 2017) to exemplify the key difference.

Permissioned blockchains are not very different from traditional databases. Private blockchains are adopted by a single organization. Conversely, a blockchain deployed across multiple organizations is called a consortium blockchain. In a consortium blockchain, pre-authorized nodes control the consensus process while the read access may be public or limited to specific participants. R3 can be a good example of a blockchain consortium. This company leads over three hundred companies engaged in the development of distributed applications on the top of Corda, called CorApp for adoption across industries, including financial services, trade finance, healthcare and digital access. Corda is an open source distributed ledger platform, which is not based on the concept of blocks containing transactions (is not properly a blockchain) but has features of blockchain, such as consensus, authentication, validity and immutability. Corda has been designed to perform complex transactions in the financial industry with restricted access to data. (R3; Bashir, 2017)

Of course, private blockchains are the most flexible in terms of configuration and inherently fast as a single organization governs and hosts the network of blockchain participants. However, there is not a real decentralization in this type of blockchain and they have been adopted for years (Schneir, 2019)— public blockchain is the real game changer.

All these types of blockchains are characterized by a blockchain platform, namely the software applied to run a blockchain, which includes: “the blockchain client software for processing nodes, the local data store for nodes, and any alternative clients to access the blockchain network.” (Xu, Weber, & Staples, M., 2019, p. 7) The client software is necessary in any blockchain to enable processing nodes to operate in the network, for transmitting, for example, transactions and creating blocks.

2.2.3. Smart Contracts and Ethereum

In addition to new kinds of blockchains, new tools enriched the DLT ecosystem. Computer programs called “smart contracts” enable the blockchain to perform more sophisticated tasks than simply recording and storing data in the form of blocks on a chain (Clack, Bakshi & Braine, 2016). Smart contracts can administer the ownership of any assets stored on a blockchain. They generally execute an order if certain conditions are met and can be employed to self-execute parts of legal contracts. However, there is an open discussion on the legality of smart contracts. I personally believe that smart contracts simply reflect a new form of contract. Different from an oral or written contract, in a smart contract the terms of a contract are codified into a computer program and self-executed. From a legal perspective, the main issue related to smart contracts is that the code is “deterministic and immutable once deployed” (Xu, Weber, & Staples, M., 2019, p. 7). Thus, there is no room for interpretation or modification of the terms of the contract. However, the smart contract might set that the code will change if certain conditions occur. In any case, the more details and instructions you write in the smart contract code, the more likely it is that your automated contract properly functions.

Smart contracts are also used to connect decentralized applications (DApps) to the blockchain. Unlike traditional applications (apps) that adopt centralized servers to store and process data, DApps use decentralized peer-to-peer networks—most DApps run on a blockchain. The idea of DApps gained popularity with Ethereum, a blockchain platform focused on the adoption of smart contracts to perform services without requiring a third party intermediary.

Ethereum is a public blockchain - the second in popularity and value after the bitcoin blockchain - launched in 2015, that runs not just “send and receive Bitcoin”, but a disparate set of instructions thanks to the employment of smart contracts. Ethereum has its own currency, Ether (ETH) and is basically a multi-services platform that adopts a public blockchain and smart contracts to offer a variety of new decentralized applications. In November 2019, there were 2,652 DApps built on Ethereum versus about 4,000 DApps in total (“2019 Dapp Market Report”, 2020). Every single operation that occurs in the Ethereum platform, which can be a transaction or the performance of a smart contract, requires some amount of gas. Ethereum gas is the unit that determines the amount of computational effort necessary to perform a specific operation. There is not a fixed price for the gas, but it depends on the network traffic having more transactions competing to be contained in a block.

Smart contracts can be combined to create a *Decentralized Autonomous Organization* (DAO), namely an organization entirely governed by smart contracts or a protocol, which are discussed in Section 3.1. (Kolber, 2018). In contrast to traditional companies, a DAO is not structured in a top-down manner, with a variety of layers of management and bureaucratic processes. In a DAO all participants agree on codified rules self-executed through smart contracts, rather than traditional legal contracts enforced by law enforcers. Some countries, for example Austria, are in favor of classifying DAOs as civil law partnerships subject to the related law.

In short, in the context of a blockchain all participants that are part of the network follow the rules self-executed by smart contracts or defined in a protocol. This enables reduced transaction costs of management, ensuring a high level of transparency.

As we will explore in Section 3.3, smart contracts can turn out to be valuable antitrust enforcement tools.

2.2.4. Blockchain Tokens

Again, blockchain is the infrastructure that enables recording and storing "virtually everything of value" (Tapscott D. & Tapscott A., 2016) in a cheaper and safer way thanks to a peer-to-peer network and cryptography. What you transfer in a blockchain is usually called a "token", hence an asset and/or right collectively controlled by a network of computers, which can be a blockchain network, or other DLT. Tokens are usually managed by smart contracts and run in a specific blockchain; they do not run across different blockchain networks. As opposed to cryptocurrencies, such as Bitcoin and Ether, tokens are usually implemented on the top of a blockchain platform through smart contracts features and not directly in the core platform of a blockchain. This means that, in contrast to tokens, cryptocurrencies are independent from a particular platform and can be used outside their native environment as a form of currency.

Usually tokens are distinguished into "utility tokens" or "security tokens." Utility tokens can include coins or user tokens that give the holder the right to utilize the network, to use products or services offered by a company, or to vote taking advantage of the network. A company usually launches an Initial Coin Offering (ICO), in which tokens are issued. Different from an Initial Public Offering (IPO), through an ICO you acquire tokens instead of stocks and these tokens rely on a blockchain rather than traditional backers with a centralized ledger.

Security tokens are very similar to traditional security - the only differences are that security tokens' ownership is confirmed through blockchain transactions and you can have fractional ownership (Shilov, 2019). Security tokens are issued through a Security Token Offering (STO), which was proposed in 2017 in the United States. Security tokens are under the supervision of the Securities and Exchange Commission (SEC) to improve the protection of investors. (Hassani, Huang, & Silva, 2019). That said, the distinction between security tokens and utility tokens, as well as an ICO and an STO, is controversial. In the USA, a token that passes the so-called "Honey Test" falls within the definition of security token and it is subject to the SEC regulation. Many developers simply call "utility tokens" something that is not to escape government regulation and taxes. (PricewaterhouseCoopers (PwC) & Crypto Valley, 2019).

2.2.5. Recent Developments in DLT

In ten years the DLT ecosystem has completely changed. As outlined above, Bitcoin blockchain is only one of the numerous blockchains now in use, which is adopted to transfer potentially everything—not only cryptocurrencies. Bitcoin blockchain is considered the first generation of blockchain technology (Blockchain 1.0) used to merely transfer cryptographic currencies, such as bitcoins. Bitcoin blockchain was a breakthrough technology. However it showed some technical limitations, especially in terms of scalability and adaptability. Bitcoin blockchain takes around ten minutes to create a new block that can accommodate approximately an average of 2700 transactions. Visa, on the other hand, performs an average of 24,000 transactions per second with a peak of about 50,000.

Ethereum led the second generation (Blockchain 2.0) with the exploitation of smart contracts, the development of DApps and token assets, including financial services. In other words, Blockchain 2.0 expanded the implementation of DLT applications for general industries, such as government, media, health, justice and the arts. Although the second generation of blockchain made the DLT eco-system more sophisticated with new tools and applications, it did not resolve the main technical limitations underlying DLT. We need to look at the third generation (Blockchain 3.0) to see some real improvements in that sense.

Blockchain 3.0 is recognized as the third generation of blockchain that has tackled the challenges raised in Blockchain 1.0 and 2.0. generations: scalability and interoperability. For example, Cardano, IOTA and Nano fall within the Blockchain 3.0. Cardano uses the Proof of Stake (PoS) protocol to solve the issues of scalability and sustainability, instead of PoW, and adds interoperability among different blockchains. PoS means that the participant in the blockchain network that can mine or validate a block is determined according to its wealth (stake). In other words, the "miner" or "validator" is selected based on how many coins it holds. This means that a miner is subject to a pre-approval, and there is no block reward, but the miner receives a transaction fee. PoS seems to be more energy-efficient as it does not require spending massive amounts of energy to resolve the computational problem required by the PoW.

Cardano adopts PoS. To improve scalability and interoperability, Cardano is developed in two layers: one for the settlement of transactions (the settlement layer) and one for computing smart contracts and DApps (computational layer). This more sophisticated architecture aims to facilitate modifications on the consensus protocol without manipulating both layers.

The issue of scalability has also been addressed through the so-called *lightning network*, which is based on a payment channel to perform transactions in a blockchain platform in a faster and cheaper way (Poon & Dryja, 2016). In short, the lightning network creates a micropayment channel that enables one to send large amounts of money to another party in a decentralized fashion. Parties pay a fee only once and can transact back and forth without paying fees to *miners*. As Poon and Dryja (2016) observed, these channels "are real bitcoin transactions", not a separate "network on top of bitcoin" (p. 4). Parties sign a balance sheet that includes each transaction; once their transactions are completed, the parties pay to close the channel ("What is Bitcoin's", 2018).

In summary, Blockchain 3.0 made blockchain infrastructure more efficient and flexible for multiple adoptions. (Bashir, 2017). It is now possible to envision a new generation of blockchain, but the innovation that will bring it about is still being investigated.

Having explored the origin, the main characteristics, and the applications related to DLT, you are now prepared to embark on the exploration of antitrust and competition as it relates to DLT.

3. DLT And For Competition

As outlined in Section 2, the diversity of DLT applications is breathtaking. From bitcoin blockchain, we now benefit from an extremely wide portfolio of DLT solutions, which compete not only with each other, but also with traditional centralized platforms (Werbach, 2018). DLTs usually offer more efficient alternatives than centralized platforms in terms of security and costs. In blockchain, the possibility of losing information is basically zero, as information is stored on a number of computers and synchronized ledger copies.

Transparency increases without compromising privacy through the adoption of encrypted systems, such as PKC, or more sophisticated mechanisms like confidential computing. Usually service providers encrypt data when data is transferred and stored; data is typically not encrypted when in use. Confidential computing aims to secure data exactly when processes in memory, hence data is in use. The Confidential Consortium Framework (CCF) is an open-source project based on Microsoft Azure Engineering that builds highly secure, available and performant applications through confidential blockchain networks (Microsoft).

Section 3 investigates blockchain and competition from two different perspectives. Section 3.2 explores how blockchain platforms can compete with present centralized online platforms that today raise the most critical issues in the context of antitrust. Twenty years ago, the Internet platform enabled markets to shift from physical platforms to digital platforms, reaching people all over the world by saving time, money and gaining in efficiency compared to physical infrastructures.

As the Internet did twenty years ago, blockchain can change markets yet again. The shift from centralized to decentralized blockchain-based platforms is likely to bring in a new era marked by this technology—the *Blockchain Era*. (Massarotto, 2020a) Section 3.3 dives into the exploration of how antitrust enforcers can exploit DLT as a tool to enforce antitrust principles with a focus on data-driven markets.

3.1. From Centralized to Decentralized Platforms

3.1.1. The Internet Centralization

Today the Internet appears to be highly centralized. Large technology companies—known as *Big Tech*—found creative ways to become necessary intermediaries between the users and the Web, which is now critically centralized. (Massarotto, 2019b) In 2020, Facebook reached 2.6 billion monthly active users (Statista, 2020) and Google Search is the undisputed leader of search engines with a worldwide market share of over eighty-seven percent (Statista, 2020b).

Similar to the end of the nineteenth century when Rockefeller, a private business man, controlled the most valuable resource—oil—today, a few corporations known as *Big Tech* control the data business, recalling the threat of private monopolies in crucial industries. (Massarotto, 2018) Data is the fuel that today runs machine-learning algorithms (MLA), which is the main application of Artificial Intelligence (AI), a business which all companies are now jumping into. As a result, the value of data has surpassed that of oil (Massarotto, 2019; Bhageshpur, 2019).

Consequently, the issue of *Big Tech* is increasingly relevant for antitrust agencies because the centralization of the Internet *de facto* restrains competition in today's most crucial industry (Massarotto, 2019). In addition, we have to consider that the same *Big Tech* are now building their own Internet infrastructure and can potentially monopolize all aspects of the Internet marketplace. Google "Curie" project is only one example (Submarine Cable Network, 2020); and blockchain relies on the Internet.

To date, the U.S. and EU antitrust agencies have shown very different approaches in dealing with digital and data-driven markets. While the U.S. antitrust enforcers are criticized for being excessively lax, the EU antitrust authorities seem to be very prone to sanction large high-tech companies for monopolizing crucial digital markets (Massarotto, 2020c). The US and EU Google cases show clearly this diversity in approach and both no antitrust action at all or heavy fines seem to be an arguable solution.

An argument here is made that DLT can effectively compete with today's centralized platform by reducing the power of *Big Tech* and restoring the Web's decentralization (Massarotto, 2020a). DLTs are decentralized by design. This means that information is distributed in a decentralized ledger where anyone (in case of public blockchains), or selected participants (in case of private and permissioned blockchains) can have access and participate in the chain (Catalini, C. & Tucker, 2018; Lianos, 2018). This is what mainly distinguishes blockchain from a traditional database (e.g. Google Drive). However, not all decentralized databases are necessarily blockchains. In 2016, for example, Sir Tim Berners Lee, the founder of the Web, introduced Solid: a project based on a decentralized platform where data of each user are stored (https://solidproject.org/). Solid promises, through its decentralized platform, to enable each user to have full control of his data and to better protect privacy. Although decentralized, Solid is not a blockchain; data are stored in "pods" and there is not a consensus mechanism to govern the Solid platform. This is why some doubt that Solid is effectively a decentralized platform (Dujmovic, J., 2018). However, projects like Solid compete with DLT and need to be considered in the discussion of DLT and competition.

Blockchain can not only promote the decentralization process of the Web, but also bypass third intermediaries, which in case of bitcoins are banks. Thus, the adoption of blockchain potentially makes present services and goods cheaper by having the same consumers/users part of the chain to benefit from network effects that one could not experience as a single individual. Anyone can create and participate in a decentralized public blockchain network, like anyone can create a buyer group to acquire some specific products bypassing, for example supermarkets (Massarotto, 2019b).

Blockchain is known for bitcoin and cryptocurrency but can be used to store and transfer everything that has a value, for example data, bypassing any kind of intermediary, including today's centralized databases. Through a blockchain, data can be stored in multiple computers, which constitute the blockchain network, by increasing security and ensuring the same access to data to all the blockchain participants. Therefore, blockchain architecture can enable each Internet user not only to have the same knowledge of data transferred through the Internet, but also to own and control potentially all its personal data stored in a blockchain. Everything is tracked in a blockchain and each user can verify and control its data anytime on the Internet through the adoption of a private key. Privacy can be better protected than existing regulation by means of PKC and confidential computing solutions (Massarotto, 2020a).

Theoretically, any regulators can exploit blockchain technologies to guarantee a transparent system that better ensures privacy and security to both companies and any consumers affected by the related industry and regulation (Massarotto, 2020a). In other words, DLT can both effectively regulate the data industry and tackle today's main antitrust concern—the Internet centralization and the monopoly power of *Big Tech* (Massarotto, 2020c). In addition, DLT increases transparency among blockchain users, potentially making any services and goods cheaper.

Today, corporations in any industry have successfully completed DLT projects and are constantly working on improving these technologies. Thus, DLT magnitude is expected to grow exponentially in the next few years by providing increasingly sophisticated solutions to companies, consumers and the same institutions.

However, as explored in Section 4, DLT need antitrust to grow and become a fundamental component of our economy. DLT are subject to anticompetitive conduct that can compromise their key characteristic—*decentralization*. DLT is not magic and should not be immune from the antitrust scrutiny to prevent engagement in anticompetitive behavior to profit beyond that attainable in open and free markets. Antitrust will be crucial in marking the transition from centralized to decentralized platforms viable (Massarotto, 2019b).

3.1.2. Is it the time for a Blockchain Era?

> "In a few years, men will be able to communicate more effectively through a machine than face to face" *J.C.R. Licklider* and *Robert Taylor*

This statement dates back not to the 1990s, but to 1968 when the pioneers of the Internet wrote "The Computer as a Communication Device" paper (Licklider, J.C.R. & Taylor, R. (1968), which set the tone for the creation of the most critical means of communication ever. Since the 1990s, the Internet though the Web has critically changed our daily life, impacting every economic sector and situation. *Will blockchain be the next cutting-edge technology that will revolutionize our economy and daily life again?*

An argument is made here that DLT has the potential to change market paradigms again, bringing us into the *Blockchain Era*. The similarities between a public blockchain and the Web are compelling and will be explored to predict the future development of the blockchain ecosystem.

Again, the creation of the Internet dates back 1968, but the real game changer was the World Wide Web (Web) in the nineties. Sir Tim Berners Lee, a computer engineer of CERN, created the Web due to his frustration to switch from one computer to another to get information. Tim Berners Lee also recounts that he often had "to learn a different program for each computer" (Licklider, J.C.R. & Taylor, R., 1968). Interoperability is the real power of the Web (Yu, P. K., 2007). In short, the Web is a set of open protocols and standards—the Hypertext Transfer Protocol (HTTP) and HyperText Markup Language (HTML)—similar to those that we have explored for blockchains. These open protocols and standards enabled a user to switch from one site to another smoothly.

Today blockchains are running on different protocols without being interconnected among each other, similar to the situation of the Internet before the advent of the Web. But in the near future the situation might change, and like Tim Berners-Lee in 1990, someone could set open and free protocols in a public blockchain that enable interoperability among different platforms. Similar to the Web, these open protocols and standards defined for blockchain could set the tone for a universal open blockchain where existing and future blockchain goods and services can run (Massarotto, 2020a; http://info.cern.ch/hypertext/WWW/TheProject.html).

The founder of the Web decided to release and make available on a royalty free-basis the code underlying the Web by recognizing that this was the reason why the Web took-off. He argued that "you can't propose something be a universal space and at the same time keep control of it" (Webfoundation (n.d.). History has later confirmed his thoughts. In the mid-90s Microsoft, for example, developed Blackbird, a proprietary version of the Web, which was offered as an alternative to HTML for a short time. Blackbird was used to run the Microsoft Network (MSN) but it was cancelled since the overwhelming adoption of the HTTP and HTML standards.

3.1.3. Blockchain Standards

The definition of blockchain standards is compelling. However, there are many issues behind the creation of these universal standards for blockchains. Ethereum, for example, created *Enterprise Ethereum Alliance (EEA)*, a member-driven standards organization connected with large corporations, including Intel, Microsoft, academics and start-ups. EEA develops open blockchain specifications to promote harmonization and interoperability for businesses and consumers worldwide. However, there are some concerns about EEA and the development of these standards, since Ethereum does not appear to be fully decentralized (Canellis, n.d.). As outlined in Section 2, the Ethereum ecosystem relies on Gas, and the decision to hard-fork the protocol in 2016 to deal with the Ethereum DAO hacker attack questions Ethereum decentralization. (Kolber, 2018; Werbach & Cornell, 2019) Therefore, the issue of interoperability among different platforms would likely remain unchanged by means of these sorts of standards. Each platform is likely to promote its own standards.

However, the issue of standardization in the context of blockchain is certainly of primary importance. There are those who envision the possibility of defining standard essential patents (SEPs) for blockchains subject to FRAND (Fair Reasonable and Non Discriminatory) licensing obligations (Sung, 2018). SEPs are defined by Standard Setting Organisations (SSOs), such as the

European Telecommunications Standards Institute (ETSI) and the Institute of Electrical and Electronic Engineers (IEEE). SSOs develop worldwide standards for information and communications technologies, including Global Systems for Mobile Communications (GSM), Wideband Code Division Multiple Access (WCDMA) and the "Wi-Fi" technologies, namely a set of standards for wireless local area networks (W-LAN) (http://www.ieee.org/about/today/at_a_glance.html). The GSM is also known as 2G technology and WCDMA as 3G technology. When a SSO defines a technology as a standard, the use of the related patent becomes essential and the patent holders agree to license the standard to anyone under the FRAND terms (Gregory Sidak, The Meaning of FRAND). The ambiguity of the term FRAND and its meaning raised the opportunity for companies to engage in patent "hold-up," often leading to costly and time-consuming litigations (Blair & Sokol, 2017). The Patent Assertion Entities (PAEs), which are companies that acquire patents but do not practice them by generating revenues through license fees, royalty and damages compensations (European Commission, *Patent Assertion Entities in Europe* (Thumm N. & Gabison G., 2016), were often accused of "patent hold-up" (Massarotto, 2016). A study conducted in 2012 revealed that Patent Assertion Entities (PAEs) litigations, which traditionally involve SEPs, corresponded to $29 billion in 2011 in the USA (Bessen & Meurer, 2014; Bharadwaj, Devaiah & Gupta, 2018); the situation looks quite similar in Europe.

This is why we need to consider with caution the adoption of this kind of standardization process in the discussion of defining standards for blockchain. In other words, we need to balance the need for interoperability among blockchain platforms with a standardization process that can lead to the risk of patent hold-up or other forms of abuse (Lianos, 2018).

Another way to define standards is through the creation of a consortium similar to W3C, which Tim Berners Lee built after designing the Web to develop new and improvements of the Web's standards and protocols. Today many entities, including Amazon, Apple, MIT, and Stanford University, have joined W3C in the development of Web standards (https://www.w3.org), which are publically available free of charge. However, this kind of standardization process also casts some doubts as some of the largest Silicon Valley corporations, including Google and Microsoft, joined the consortium by recommending debatable standards, such as the EME (Halpin, 2017).

Standardization is usually developed when a technology reaches a mature stadium to decrease switching costs. In its third generation we can confidently argue that today, blockchain is a mature technology. The issue of blockchain standards will certainly be one of the most critical in the development of DLT. Antitrust enforcers should oversee the standardization process, providing any feedback. Many antitrust cases related to information technology (IT), such as Microsoft and Intel, concerned the issue of interoperability and patent licensing. There is much to learn that we can use from previous IT antitrust cases in the development of blockchain.

Blockchain can revolutionize our daily life like the Internet did twenty years ago. Alternatively, as Prof. Werback (2018) observed, blockchain will be "just the way that all organizations eventually do what they do more efficiently" (p. 3).

3.3. DLT as Antitrust Tool

DLT, in particular blockchain and smart contracts, can turn out to be a valuable tool to enforce antitrust law by improving the antitrust enforcement from different aspects. For example, one of the primary antitrust concerns is related to the costs associated with monitoring companies' compliance with antitrust remedies. These remedies, which most of the time are enshrined in antitrust consent decisions, can be automated by means of smart contracts. (Massarotto, 2019; OECD, 2018)

Not all smart contracts need to or can necessarily be automated, but certainly many of them do. For example, in August 2010 the Federal Trade Commission (FTC) settled the Intel case with a consent decree (FTC, 2010), which imposed on Intel to:

- "extend Via's x86 licensing agreement for five years" which would have otherwise expired in 2013;
- "maintain a key interface, known as the PCI Express Bus, for at least six years in a way that will not limit the performance of graphics processing chips." (FTC, 2010).

These remedies can be easily translated in a computer code that is enforced by a program. A smart contract can automatize the compliance of the companies with antitrust remedies by automatically punishing company's deviation from compliance (Massarotto, 2019a). This would significantly decrease the costs incurred by the antitrust agency in monitoring the remedies imposed. Moreover, antitrust agencies can better monitor companies' compliance with antitrust remedies by releasing the company from filing extensive Reports to the agency, which are usually required for companies every six months or so. Perhaps, a wide adoption of smart contracts would raise the risk of bugs and hacker attacks, and this is certainly something that the enforcers need to consider in adopting smart contracts (Dingman, Cohen, Ferrara, Lynch, Jasinski, Black & Deng, 2019). Smart contracts could also be implemented in advance to ensure blockchain compliance with antitrust and any other affected regulations.

As I suggested in my book "Antitrust Settlements: How a Simple Agreement Can Drive the Economy" these smart contracts can run in an antitrust blockchain made up by antitrust officers, where potentially, each officer or division/department represents a node. This antitrust blockchain could be built for one specific or multiple agencies. For example, a European antitrust blockchain network might be ideal to enhance communication and harmonize the enforcement of competition principles among the European Member States. Each European agency might have its own blockchain connected to the European Antitrust Blockchain.

In practice, what antitrust authorities could explore is the adoption of smart contracts that run on a blockchain network base, for example, on the Hyperledger Fabric DLT platform. The antitrust agency's smart contracts would require privileged access to all transactions on the ledger, monitor all transactions, and produce compliance reports. Companies may be granted read-only access to those aspects of the reports related to their activities.

Antitrust agencies may also require companies that raise antitrust concerns to adopt pro-competitive remedies which may include the implementation of a blockchain to track the data flow and enable the antitrust agency to oversee the company's use of data (Massarotto, 2020c).

In summary, antitrust discipline can find a variety of situations and ways to exploit DLT in enforcing antitrust principles in any markets. The adoption of cutting edge technologies in the context of antitrust is not merely recommended, but it seems to be essential to ensure effective antitrust enforcement in today's tech-economy.

3.4. Conclusions

In the context of antitrust, as well as in any field, DLT offers a variety of opportunities for antitrust enforcers. As explored in this Section, DLT seems to be all what antitrust dreams about: a tool to effectively decentralize today's consolidated platforms on the Web and regulate data by ensuring privacy in a more efficient way than existing regulations. Antitrust enforcers should not miss the opportunities that these cutting-edge technologies offer to face its present challenges in the tech-economy. There is essentially no chance that an antitrust agency can effectively face today's challenges in increasingly dynamic and high-sophisticated markets without exploiting the same *Big-tech* ingenuity (Massarotto, 2020c).

4. Do Blockchain Raise Antitrust Concerns?

Antitrust practices are present in the context of blockchain and can seriously compromise the key component of blockchain—*decentralization*. Similar to the Web, blockchain originated as a decentralized and open network, but anticompetitive conduct can lead to centralized blockchain's governance, jeopardizing blockchain's future development.

In this section we will explore:

1) the meaning of trust in trustless technologies;
2) what kind of entity blockchain is;
3) forms of collusion;
4) the issue of market concentration;
5) exclusionary conduct.

All these issues are fundamental and need to be considered in the development of blockchain. If decentralization is compromised through collusion and market concentration and/or exclusionary conduct, blockchain will become only another centralized platform adding no concrete extra value to the existing platforms.

4.1. Anti-trust in Trustless Technologies

The word *trust* appears frequently in the context of blockchain. We often hear that blockchain is a trustless technology. But the meaning of trust in the blockchain ecosystem seems to be controversial. The issue dealing with antitrust is particularly intriguing, as this discipline centers around the word *trust*.

This Section 4.1 investigates the meaning of *trust* exploring whether the so-called trustless blockchain technology should be immune from the antitrust scrutiny. In contrast to centralized platforms, in public blockchain you do not need to trust a third party intermediary (e.g. banks) by using a blockchain. In his white paper, Satoshi Nakamoto claimed to have introduced "a system for electronic transaction without relying on trust," potentially making bitcoin and blockchain immune from the antitrust scrutiny (Nakamoto, 2008). Thus, at the first glance someone could argue that blockchain is exempted from antitrust surveillance.

However, Satoshi Nakamoto's claim is not entirely true. The peer-to-peer network bypasses centralized platforms, but its functioning relies on the network of participants in the chain, which (as explained in Section 2.2) is governed by a protocol. In other words, you need to trust the technology and who set the protocol, instead of an intermediary (Shein, 2019). The success of blockchain relies on the trust of people in this new technology: blockchain and DLT in general is not an exception to this fundamental economic principle (Massarotto, 2020).

The truth is that the agreed algorithm protocol establishes mutual trust among the participants in the network by validating transactions based on a peer-to-peer mechanism (Puthal, Malik, Mohanty, Kougianos & Yang, 2018). This means lowering the costs of checking digital information, though the cost of verifying offline information remains the same. Professor Kevin Werback observed that bitcoin and blockchain do not eliminate *trust*, but they introduced a new form of *trust* by inverting the problem. People "make payments confidently with a decentralized digital currency" because they "pay people with it" (Werbach, 2018). Professor Werback defined a fourth structure of trust in blockchain.

I personally believe that *trust* is always the same *trust*, from cryptocurrencies to the context of antitrust. What does change is the context where this term is employed that can significantly change its meaning. Rather than trusting your competitor from not competing with you, or the government and judges for correctly enforcing the rules, or a bank for keeping your money safe, you trust the technology—the protocol (Schneir, 2019). This brings us back to the cryptoanarchy movement. You adopt a blockchain and you buy bitcoins because you trust a computer protocol more than the bank system and the government's regulation.

If something goes wrong, bitcoin protocol enables the majority of the network to create a fork to reverse the consequences of hacking or bugs. The possibility to fork a blockchain keeps blockchains constantly under competitive pressure. In case a fork "offers better governance or is more competitive, it will quickly gather users and developers since switching costs are extremely low" (p. 8). This does not occur in private and permissioned blockchains, where there is not a real decentralized platform; they are very similar to traditional databases.

Up until May 2020, there were three hard forks in the bitcoin network (Bitcoin XT, Bitcoin Classic and Bitcoin Unlimited), but none reached the consensus, namely the majority of hash power. In 2016, a hard fork succeeded in Ethereum to repair the failure of '*The DAO'* launched in Ethereum platform. At that time, the world seemed to be ready for a venture capital firm entirely self-governed by a smart contract running on a blockchain—Ethereum. The enthusiasm was so high that DAO raised $150 million in only a few months.

Unfortunately, a project aimed to be remained in the history for proving the validity of DAO, is now the symbol of a tremendous failure. A bug in its smart contract enabled a hacker to drain about $ 50 million. Some blockchain purists argued that this was part of the game and the hacker just performed something that the computer code permitted (Kolber, 2018). However, Ethereum opted to fork its blockchain and the fork successfully created Ethereum classic, which maintains the original blockchain, and the new Ethereum with the theft reversed (Leising, 2017).

This episode certainly led many to distrust DAO, and DLT, confirming that these technologies are not immune from the economic principle of *trust*. In the history of bitcoin and blockchain, *The DAO* of 2016 is not the only episode that discouraged people from investing in DLT. Silkroad and BitInstant are other two symbolic examples of how these technologies can be used to commit or incentivize crimes, such as money laundry, selling drugs, and other illegal goods and services on the Web (Planet Compliance, 2017). These episodes seriously affected the reputation of bitcoin and the DLT ecosystem. The price of Bitcoin, for example, dropped from 140$ to 110$ after the FBI shouted Silk Road, the website for selling drugs administered by Ross Ulbrich, where all transactions were conducted using bitcoins (Hern, 2013; "Bitcoin value drop", 2013).

Likewise, DLT is not trustless from an antitrust perspective. As explored in the following Section 4, some types of blockchain may create the perfect conditions for companies to collude. Moreover, as previously observed, participants need to trust each other, raising the issue of whether this might imply some sort of collusive conduct among blockchain participants that is relevant for antitrust scrutiny.

In summary, the magnitude of DLT is enormous, but like any promising technology, DLT can be used for enabling people and markets to do what they do more efficiently, or creating more harm than benefit. DLT requires trust in order to increase its reputation and attract business. We are living in a reputation-based system—today, the economic principle of *trust* is even more relevant.

We commonly hear the slogan: "Don't trust anyone with more money that their reputation is worth" (Schneir, 2019b). Reputation will be far more important in dealing than ever the credit ranking now (Schneir, 2019b)—blockchain marketplace is the next testing ground.

Antitrust and effective forms of regulation will be critical to increase the reputation of the market and build—*trust*—in DLT as well as in any markets (Zak , 2017; Massarotto, 2020a). On the other hand, the adoption of blockchain technologies by the same government agencies might increase cryptoanarchy purists' trust in government's regulation.

In any case, antitrust and DLT should play in the same team by pursuing an identical goal: increasing consumer welfare by advancing markets through cutting-edge technologies. They can only benefit from mutual assistance. (Massarotto, 2020a).

4.2. What Kind of Entity is Blockchain?

Before exploring possible antitrust concerns, it is worth investigating blockchain's identity in order to verify if this entity can be directly liable for antitrust violations. Antitrust presumes that there is a defined entity or a set of entities that aim to market power, which in case of monopolization, conduct or agreements in restraint of trade, can be investigated. Otherwise, as Professors Catalini and Tucker observed, it is basically impossible to prosecute antitrust conduct in the context of blockchain. (Catalini, C. & Tucker, 2018; Lianos, 2018)

Should blockchain be considered as a firm, or a network that enables people and companies to interact or something different? The decentralized nature of blockchain can, as we have seen, help antitrust agencies in preserving competition in today's centralized platforms. On the other hand, the inherent decentralization of blockchain brings new challenges for antitrust enforcers in terms of defining blockchain's identity.

Similar to the nineteenth century, where society created corporations to separate people from entities devoted to business, a decade ago it introduced a new decentralized entity/infrastructure to operate. Differently from traditional corporations, in decentralized blockchains, people participate and interact with the blockchain network through a digital identity.

Digital identity can be identified as "the digital data corpus being built by users and digital systems" (Fehér, K., 2019) that enable people and any other entity to access computers and interact with computer networks. Blockchain is a decentralized computer network and in public blockchain, such as bitcoin blockchain, people's digital identity is characterized by pseudonyms to protect privacy. The same creator of bitcoin is still known under the pseudonym of Satoshi Nakamoto, no one was able to reveal his real identity.

Satoshi Nakamoto is likely to be only one of the several pseudonyms that the founder of bitcoin uses to interact on the Internet. There is often the wrong assumption that we have only a digital identity that follows us everywhere; but this is basically not true. Every day, we create, for example, a number of email and social media accounts. Digital identity is different from our passport or social security number, and it is naïve to think that we should have only one digital identity (Ou, 2017). Similar to corporations that were created as a separate entity from its owners, digital identity is something separate (although related) to its creator.

In other words, blockchain creates a network made up by blockchain participants who interact with each other by using digital identities. Blockchain is basically the platform that enables people to interact to do much of their regular work more efficiently bypassing intermediaries. Similar to a buyer group, as we have seen, participants in the blockchain group/network are basically users that leverage their force of acting together to get goods and services that are usually provided through intermediaries.

Thus, what kind of entity is blockchain? A deeper inquiry is necessary, but as any group such as associations, consortiums or networks, blockchain does not appear immune from antitrust scrutiny. By considering the US and EU competition law, which are the main antitrust jurisdictions, we can observe that antitrust law is giving an increasing importance to the economic effects of practices in the affected markets, rather than formalistic legal definitions of entities relevant for antitrust legislation. The US antitrust law clearly emphasizes this point as under Section 7 of the Sherman Act, antitrust law is applicable to potentially any "person," including "corporations and associations existing under or authorized by the laws" (Section 7 of the Sherman Act). In Europe, Article 101 and 102 of the TFEU applies to undertakings and associations, which exercise an economic activity (Lianos, 2018). Therefore, blockchain can easily fall into both the US and EU antitrust jurisdictions.

As outlined above, a set of rules set into a protocol governs the blockchain network. But, a group of people wrote the protocol and is leading the blockchain growth. The fact that these people are using digital identities does not make them less liable.

4.3. Forms of Collusion

In the context of blockchain, one of the main antitrust issues entails collusive practices among participants or different blockchain networks. If this concern takes place, the subsequent issue is whether antitrust agencies should prosecute blockchains and in which way.

First, in this discussion it is necessary to treat private, permissioned and public blockchains separately.

4.3.1 Private and Consortium Blockchains

Private blockchains are not so different from traditional databases; for these reasons some scholars considered them "100 percent uninteresting," (Schneir, 2019a) because they have been used for years. They are closed networks; blockchain participants need to be invited and are only known to each other (Jacobs, 2018). In other words, participation occurs by invitation only, and everything that happens within is totally private.

As outlined in Section 2, while usually singular organizations take part in private blockchains, consortium/federated blockchains include multiple selected organizations. If a blockchain consortium is built among competitors to exchange sensitive information, such as prices, they are dangerous in terms of competition as much as any other consortium/organization associated with that scope. Decisions are taken through a voting or multi-party consensus algorithm whose rules rely on the agreement of the participants set in the protocol that governs the blockchain network. For example, a consortium of fifty organizations could rule that a transaction is only added to the blockchain if more than thirty-five organizations part of the consortium have validated the transaction. The main differences between a traditional consortium and blockchain consortium is the adoption of an infrastructure to communicate and the possibility to automate tasks with the use of smart contracts, which might be adopted to detect and punish a cartel deviation, making the cartel more effective.

However, if the antitrust agency wants to participate in the blockchain process to verify the lawful compliance of participants, the possibility that the agency would detect any forms of collusion if very high as everything is tracked in a blockchain and immutable (Massarotto, 2019b). Thus, if on one hand, companies can engage in collusive conduct more efficiently by adopting smart contracts, on the other hand, any forms of collusion can be easily proved. As I have written in my paper "From Digital to Blockchain Markets—What Role for Antitrust and Regulation," antitrust agencies or regulators might think of setting some standard rules or conditions hardcoded in *smart contracts* to automatically punish forms of collusion. *Smart contracts* have the potential to become a remarkable legal and antitrust tool.

In summary, blockchain and smart contracts seem to be a double-edged sword for companies that want to collude with each other. A natural question is whether a company should use blockchain to collude when the proof of collusion would become easy to get for antitrust enforcers. Even today, meeting in a restaurant or hotel rooms seems to be the most effective and convenient ways for companies to engage in cartels and collusive practices. Especially, if antitrust agencies start adopting the same blockchain technologies to do what they regularly do.

4.3.2. Public Blockchain

The discussion of collusion in public blockchains is much more compelling. Public blockchains are intellectually stimulating because they resolved the so-called *Byzantine Generals' Problem* related to distributed networks. Computer scientists studied for years how to reach a consensus among different computers in distributed systems by considering the fact that some computers might not tell the truth. Until the advert of blockchain, no viable solutions were found to resolve such a problem. When the 2008 Satoshi Nakamoto white paper was announced, the entire computer science community was amazed.

The ingenuity of blockchain was to define a consensus algorithm according to which participants in the network need to agree to a set of protocols and rules to achieve the consensus. Similar to a game, the consensus mechanism works as long as the majority of participants in the network follow the rules hardcoded into a protocol. If everybody follows the rules, everybody wins. As explored in Section 2, bitcoin blockchain adopts the PoW to reach the consensus in the network and validate the transaction, while for example Cardano uses the PoS.

Professors Cong and Zhiguo (2019) observed that "achieving [the] consensus requires sufficiently distributing information for verification;" (p. 1755) this increases transparency potentially leading to collusive practices. However, as the Organisation for Economic Co-operation and Development (OECD) observed, the transparency of price information can increase consumer welfare (OECD, 2018). For example, the ride sharing company Uber developed a pricing algorithm that matches drivers to consumers seeking rides by employing a real-time pricing algorithm. A study estimated that this algorithm generated a consumer surplus of $ 2.9 billion in four U.S. cities (Cohen, Hahn & Hall, 2016).

In addition, everybody sees everything in a public blockchain, which is open to any person interested in joining the network. This implies that forms of cartel among blockchain participants do not seem to be an issue as the secrecy of a cartel here fails and the number of blockchain participants is subject to change constantly.

The real antitrust concern in public blockchains are mining pools, hence participants that pool together their computing power to resolve the puzzle required in PoW and increase the possibility of adding a block and be rewarded. If the block is successfully mined, the pool manager distributes the coinbase transaction to reward the group of miners who participated in forging the block (Ren &Ward, 2019). Usually each participant receives a flat fee or the award is based on the amount of computing resources used to solve the hash problem. (Bashir, 2017; Cong, He & Li, 2018)

There are also mining services contracts that you can purchase though easy-to-use web interface or the cloud (Bashir, 2017). You buy, for example, some share of mining power from cloud mining and you profit along with the pool without the need of owning mining hardware. The two main types of cloud mining are: hardware leasing and hashing power leasing. In the first type you rent their miner for a determinate amount of time, while hashing leasing means renting a specific amount of processing power. Cloud mining diverges from mining pools because in cloud mining you pay a service provider that mine for you to get the rewards. In mining pools miners share their computational power to mine blocks and gain rewards. However, also cloud mining can give rise to antitrust concerns as they imply a concentration of power in a single cloud.

In summary, mining pools and cloud mining can *de facto* lead to anticompetitive practices as they are becoming increasingly popular in the context of blockchain. A study determined that within four months the percentage of pool-mined blocks "increased from 49.91% to 91.12%" in Bitcoin and "from 76.9% to 92.2%" (Ren &Ward, 2019) in Ethereum. In other words, mining pools hold more than ninety percent of the entire blocks production in the two largest blockchain. In addition, mining pools might be attempted to collude and engage in cartels acting as a monopoly pool that controls the blockchain network. In May 2019, four mining pools were controlling more than fifty percent of the hash rate of the Bitcoin blockchain, by implying that if they get together these mining pools could successfully perform fifty-one percent attacks of the

Bitcoin network (Medium, 2019). The hash rate is "the measuring unit of the processing power of the Bitcoin network," (Bitcoin.org) Antpool alone holds about fifteen percent of the entire hash rate of all Bicoin mining pools used to mine Bitcoin (Blockchain.com). Bitmain Technologies Ltd. (Bitmain), which is the largest Bitcoin hardware manufacturer worldwide, runs Antpool. In 2018, United American Corp. sued Bitmain for antitrust violations before the U.S. Court of South of Florida (Case No. 1-18-cv-25106 (S.D. Fla)).

4.3.4. United American Corp v. Bitmain

United American Corp. v. Bitmain is the first antitrust blockchain dispute in the context of blockchain. Although up to the writing of this chapter the case is still pending, it is interesting to examine the potential antitrust issues involved and the United American Corp. (UnitedCorp) allegations. In November 2018, Bitcoin Cash, which is one of the varieties of permissionless cryptocurrencies, was forked into Bitcoin SV and Bitcoin ABC. According to UnitedCorp, Bitmain colluded with a number of investors and mining pools to get enough miners to support Bitcoin ABC over the Bitcoin SV version of Bitcoin Cash. By doing so, Bitmain would have "centralized what is intended to be a decentralized transactional system enabling the corruption of the democratic and neutral principles of the Bitcoin Cash network" (*United American Corp. v. Bitmain, Inc*., 2018). This would have compromised the value of both forks of Bitcoin Cash, which fell below the value of united Bitcoin Cash before the forking by causing financial harm to investors. In particular, United Corp's investments in Bitcoin Cash were seriously compromised due to the manipulation of the cryptocurrency market for Bitcoin Cash. The first question we should ask is whether United Corp was directly harmed by the alleged conduct. United Corp did not specify in its complaint whether it was harmed as an investor, a miner or as a spender of Bitcoin Cash.

The complaint appears quite vague also with respect to the antitrust injury that United Corp would have suffered. Bitcoin Cash's devaluation seems to be the only possible valid allegations that could effectively harm consumers. But, in that case it seems unlikely that a judge recognizes a direct harm of UnitedCorp. In sum, from an antitrust perspective, the case at hand seems to be weak on many levels.

Although cryptocurrencies and blockchains are based on the concept of decentralization, there is nothing that goes against possible agreements among participants to pool their computational power or stakes, for example, to attack the blockchain and create a fork. Conversely, the possibility to fork a blockchain increases competition by keeping blockchains constantly under competitive pressure (Catalini, C. & Tucker, 2018). Again, a public blockchain like Bitcoin Cash is based on a consensus mechanism that requires that the majority of blockchain participants agree on a common solution before adding a new block. This means that *bad participant(s)* or 'traitors' of the related blockchain network to succeed in an attack need the consensus of fifty-one percent of the participants in the network. The US cryptographer and legal scholar Nick Szabo calls this '*democracy in action*,' rather than an attack and he is probably right.

In addition, we need to consider that the mining pool itself does not necessarily own the hash power needed to mine for example Bitcoin or Bitcoin Cash. Bitcoin miners can easily switch mining pools by routing their hash power towards a different mining pool. This means that the market share of mining pools is subject to change constantly (Tuwiner, 2020). Mining pools, such as Antpool, are open and free; thus, anyone can join and leave the mining pool anytime.

In summary, *UnitedCorp v. Bitmain* is certainly an antitrust case of primary importance for the entire blockchain and cryptocurrency's community. However, on February 5th the Southern District Court of Florida dismissed the case without prejudice allowing the plaintiff to amend the complaint by no later than February 28, 2020 (Baker, 2020). United American Corp.'s amended complaint continues to claim the violation of the Sherman Act, but abandoned all five of its state law claims and it will be compelling to see the judge's ruling. This case has the potential to set the tone for future blockchain and cryptocurrencies antitrust issues.

4.3.5. Delegate Proof of Stake (DPS)

In the context of public blockchains, forms of collusion and cartels were identified in blockchains that adopted the delegate proof of stake (DPS) consensus algorithm. As previously discussed, over the last ten years blockchain engineers developed new consensus mechanisms to tackle technical challenges raised by the PoW, in particular the issue of blockchain scalability and the speed in processing transactions.

A blockchain engineer designed the DPS consensus mechanism, where blockchain participants vote the validator nodes (delegates) that will forge blocks for the chain. Each participant holds at least a token and one token corresponds to one vote. In theory, the DPS should encourage competition because users vote for people they trust more. However, in practice this consensus mechanism led in some situations to clear forms of collusion and cartels. The most notable case is probably *Lisk*, where basically two cartels ran the blockchain by producing eighty-five percent of blocks (Günther, 2018). Similarly EOS, which adopts a DPS consensus mechanism, was accused of collusion and to be controlled by a "Chinese oligarchy" (Dale, 2019).

In conclusion, forms of collusion are present in the context of blockchain and need to be prevented in order to enable blockchain maintain its key characteristic—*decentralization*. Antitrust surveillance will be increasingly crucial and necessary in the blockchain eco-system, not only to prevent forms of collusion, but also any forms of re-centralization and exclusionary conduct.

4.4 Blockchain Concentration

Blockchain is decentralized by design, implying that a number of computers (the so-called validating nodes) constitute the blockchain network. The same Blockchain's creator requires that no single entity shall control more than fifty-one percent of global computational power for Bitcoins to function appropriately. (Nakamoto, 2008)

In principle, anyone can create and participate in a decentralized public blockchain network; the more validating nodes a blockchain has, the more securer a blockchain is (Orcutt, 2018). As previously discussed, this peer-to-peer network has the potential to become universally adopted, as the Internet (more accurately the Web) is today (Lee, n.d). However, blockchain is far from being perfect.

4.4.1. ASICs

The risk of centralization, as we have seen, is effective. Today, mining bitcoins is basically impossible for a single desktop computer (Lianos, 2018), because the increase in value of bitcoins let to the development of more powerful hashing hardware. Powerful hardware called Application Specific Integrated Circuits (ASICs) can execute billions of hash per second. There are professional mining centers that today adopt thousands of ASIC units in parallel giving to users the possibility to contract with them to perform mining on their behalf (Bashir, 2017).

Today, the attempt to mine without an ASIC is unprofitable and led to the formation of the so-called *mining farms* that are usually run by corporations based in Countries with access to low-cost electricity, such as China. The same crypto purists recognized that ASIC Mining farms can lead to re-centralized the blockchain network because people cannot compete individually with ASIC farms in the mining competition (Beikverdi, Song, 2015). In addition, this has created a dependency on Bitmain, a dominant chip/ASICs manufacturer, which became a kind of third-party intermediary. This clearly goes against the same concept of a decentralized trustless technology created exactly to bypass intermediaries.

The blockchain community have created ASIC-resistant proof-of-work (PoW) algorithms that alter the required extra memory-based computing effort in response to the ASIC's threat. Ethereum, for example, introduced Ethash, the ASIC-resistant PoW. However, in concrete terms it has not resolved the problem since "chipmakers seem to be increasingly designing ASICs worthless again" (Casey, 2018). In April 2018, Bitmain announced the first ASIC miners for Ethash.

Bran Cohen, the author of the peer-to-peer BitTorrent protocol recognized that "ASIC resistance just creates more centralization around manufacture when it inevitably fails," (Cant, 2019) and it makes more sense to be ASIC-friendly. ASICs advance security thanks to their efficient hashing power that makes a potential "fifty-percent attacker" more challenging. In other words, ASICs are not entirely negative but they *de facto* increase the hash rate concentration raising antitrust concerns (Cong, He & Li, 2018).

The same blockchain community widely recognizes that the hash rate is extremely centralized and this is one of the main challenges for the development of the blockchain ecosystem (Corallo, 2019). P2Pool is a decentralized Bitcoin mining pool devised to tackle the problem of centralized mining. Similarly, Stratum V2 is a protocol for pooled mining that aims to improve decentralization through a system that enables miners to choose their own transaction sets by means of a negotiation process with pools. However, mining pools like P2Pool and Stratum V2 protocol are small realities compared with AntPool or F2Pool. In addition, P2Pool and Stratum V2 protocols are not simple tasks for non-technical users to learn.

4.4.2. Vertical concentration

In the discussion of blockchain concentration, we need to consider possible vertical concentration along the value chain of bitcoin mining (Cong, He & Li, 2018). Bitmain, as we have seen, runs Antpool one of the largest bitcoin mining pools, in addition to being the largest worldwide Bitcoin hardware manufacturer. Companies like Bitmain risks to monopolize all aspects of the Bitcoin marketplace: antitrust agencies should consider such risks.

About eighty percent of cryptocurrencies users use intermediaries, such as Coinbase, to custody their cryptocurrencies (Werbach, 2018). Coinbase is another example of centralization as it is the most successful Bitcoin wallet that has a clear centralized structure (Beikverdi & Song, 2015). Coinbase is very similar to payment platforms, such as PayPall, that controls your information with the possibility to block a client that does not follow its rules. Blockchains, such as Cardano, are also criticized for being centralized as few participants hold more than seventy percent of all Cardano coin ADA's total supply (Medium, 2019).

In summary, the re-centralization and concentration phenomena in blockchain is effective and leads to both antitrust and security issues. Moreover, if the decentralization fails, there are no many reasons why someone should prefer blockchain from any other database.

4.5. Exclusionary conduct

In case blockchain platforms become dominant and deliver essential goods or services for other blockchains or services, we have to consider the performance of possible exclusionary conduct relevant for antitrust. Exclusionary practices include: refusal to deal, tying or bundling, loyalty discounts, predatory practices. Exclusionary behaviors do not seem to be an issue in public blockchains, which are open to anybody; while exclusionary conduct can represent an effective threat in closed blockchains where participation is by invitation only.

In case a closed blockchain abuses its dominant position in a market, the antitrust agency might think of imposing remedies to tackle exclusionary behaviors. The antitrust agency, for example, might require the blockchain to break up into different parts. Or, rather, similar to the context of standard essential patents (SEP), antitrust agencies could require the blockchain to open its membership for non-participants on fair, reasonable and non-discriminatory conditions (FRAND terms). (Nazzini, 2018; Finney, 2018)

In previous antitrust cases related to exclusionary conduct, the agency prevented, for example, the company from entering into specific business or engaged in loyalty discounts. In *Intel*, which is a leading case on exclusionary conduct, the Federal Trade Commission (FTC, 2010) required Intel to:

> (1) 'modify its intellectual property agreements with AMD, Nvidia, and Via [three of its major competitors] so that those companies have more freedom to consider mergers or joint ventures with other companies, without the threat of being sued by Intel for patent infringement;'
>
> (2) 'extend Via's x86 licensing agreement for five years, which would have otherwise expired in 2013;'
>
> (3) 'maintain a key interface (PCI Express bus) for six years in a way that would not limit the performance of geographic processing chips;'
>
> (4) 'disclose to software developers that Intel computer compilers discriminate between Intel chips and non-Intel chips, and that they may not register all the features of non-Intel chips.'

In IBM *unbundling decision*, the Department of Justice (DOJ) required IBM to sell its hardware and software separately, allowing software development companies to enter the operating systems and compete with IBM (Lopatka, 2000). At that time, IBM held seventy-four percent of the market of general-purpose digital computers. The IBM unbundling decision led to the creation of the operating systems market; a start-up called Microsoft became in the 1980s IBM main supplier (Massarotto, 2020a).

At this moment it might be difficult to elaborate specific remedies for exclusionary conduct in blockchains that we cannot even envisage, but past antitrust cases can certainly be used as a useful model of reference to anticipate future antitrust remedies in the context of blockchain. Antitrust agencies could also provide some guidance to markets to prevent possible exclusionary conduct and any other anticompetitive practices in the context of blockchain. (Massarotto, 2019b) Companies are typically risk-adverse. "[T]he best of all monopoly profits is a quiet life" John Hicks (1935) wisely observed; thus especially large blockchains would benefit from government guidance.

5. Conclusions

In the 1990s, May (1994) admitted that "a lot of work remains," but the cryptoanarchy movement will soon colonize cyberspace. A question we should ask is whether blockchain will make this possible. According to the cryptoanarchy movement, when you have an idea just put into place, not wait for regulatory feedback as regulation would always limit/delay innovation (*See* Napster or BiTorrent and the same bitcoin). When a technology becomes widespread it is basically impossible for the regulator to impede its entry in the market and development. Due to network effects, a successful technology would take off with no chance to turn it down. However, there are examples like Napster or Facebook original project of Libra that show the contrary. In June 2019 Facebook in partnership with a variety of relevant partners, such as PayPal and Visa, launched its cryptocurrency Libra that has never taken off. The current Facebook Libra project is nothing more than a version of PayPal for cryptocurrency (Popper, N. & Isaac). Similarly, Telegram has to drop Telegram Open Network (TON) blockchain project after the U.S. Securities and Exchange Commission (SEC) won the injunction to prevent Telegram blockchain launch (Frankel, 2020).

In summary, DLT is not immune from government forms of regulation, including antitrust. The lack of considering antitrust and other forms of regulation can make a project illegal, therefore unsalable, in the market before it is launched. Antitrust is the first arm of government regulation that anyone needs to consider before entering into the blockchain business since this discipline is applied to any industries and situations (Massarotto, 2018).

Blockchain needs antitrust to succeed, as well as antitrust needs to embrace blockchain technologies to be effective in today's data economy. The anarchy movement is only partially right. Technologies can certainly deal with some issues in a more efficient way than present regulations, but we cannot leave humans completely out of the equation. The re-centralization of the blockchain phenomenon is only one symbolic example.

Neither overregulation nor self-regulation (anarchy) seems to be ideal. As the "security guru" Professor Bruce Schrneir (2019) observed, "markets don't take society into account" and "can't resolve collective problems" (Schneir, 2019b). The government does.

Antitrust has consumer welfare and the increase of market efficiency as primary goals. But, technologies run faster than policies. Embracing frontier technologies like blockchain is not only encouraged, but also necessary if the government wants to protect society by fostering innovation. Otherwise, it will only be a matter of time for the cryptoanarchy movement to reach the right momentum.

References

1. 2019 Dapp Market Report (2020). *Dapp Review*. Retrieved from https://dapp.review/article/238/2019-Dapp-Market-Report.

2. Baker, P. (February 5, 2020). US Judge Dismisses Bitcoin Cash 'Hijack' Lawsuit Against Bitmain, Kraken. *Coindesk*. Retrieved from https://www.coindesk.com/us-judge-dismisses-bitcoin-cash-hijack-lawsuit-against-bitmain-kraken.

3. Bashir, I. (2017). *Mastering Blockchain Distributed ledgers, decentralization and smart contracts explained*. Birmingham-Mumbai: Packt.

4. Beikverdi, A. & Song, J. (2015). Trend of Centralization in Bitcoin's Distributed Network. *IEEE*. Retrieved from https://ieeexplore.ieee.org/document/7176229.

5. Bessen J. & Meurer M. J. (2014). The Direct Costs from NPE Disputes, *Cornell Law Review, 99* (2), 387-424. Retrieved from http://scholarship.law.cornell.edu/clr/vol99/iss2/3.

6. Bhageshpur, K. (November 15, 2019). Data Is The New Oil -- And That's A Good Thing. *Forbes*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/#298c5d127304.

7. Bharadwaj, A., Devaiah, V. H. & Gupta, I. (2018). *Complications and Quandaries in the ICT Sector: Standard Essential Patents*. Springer.

8. Bitcoin value drops after FBI shuts Silk Road drugs site. (2013, October 3). BBC News. Retrieved from https://www.bbc.com/news/technology-24381847.

9. Bitcoin.org. Vocabulary, Hash Rate. Retrieved from May 26, 2020 https://bitcoin.org/en/vocabulary#hash-rate.

10. Blair, R. D. & Sokol, D. D. (2017). *Antitrust Intellectual Property, and High Tech*. Cambridge University Press.

11. Blockchain.com. Hashrate Distribution. Retrieved from https://www.blockchain.com/charts/pools.

12. Canellis, D., (n.d.). *More than 60% of Ethereum nodes run in the cloud, mostly on Amazon Web Services. Is this decentralisation?*. Retrieved from https://thenextweb.com/hardfork/2019/09/23/ethereum-nodes-cloud-services-amazon-web-services-blockchain-hosted-decentralization/.

13. Cant, J. (2019, November 16). BitTorrent Creator Calls Vitalik's ASIC-Resistant Proof-of-Work "A Pipe Dream And a Bad Idea". *Cointelegraph*. Retrieved from https://cointelegraph.com/news/bittorrent-creator-calls-vitaliks-asic-resistant-proof-of-work-a-pipe-dream-and-a-bad-idea.

14. Casey, M. J. (2018, May 1). Crypto Needs More Than Code to Beat the ASIC Mining Threat. *Coindesk*. Retrieved from https://www.coindesk.com/bitcoin-code-defend-against-asic-mining-threat.

15. Catalini C. & Tucker C. (2018). *Antitrust and Costless Verification: An Optimistic and a Pessimistic View of the Implications of Blockchain Technology*. Retrieved from http://ide.mit.edu/sites/default/files/publications/SSRN-id3199453.pdf.

16. Clack, C. D., Bakshi, V. A. & Braine L. (2016). *Smart Contract Templates: foundations, design landscape and research directions*. Retrieved from https://arxiv.org/pdf/1608.00771v3.pdf.

17. Cohen, P., Hahn R. & Hall, J. (2016, August 30), *Using Big Data to Estimate Consumer Surplus: The Case of Uber*. Retrieved from https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0048-d-0124-155312.pdf.

18. Cong, L. W. & He, Z. (2019). Blockchain Disruption and Smart Contracts. *The Review of Financial Studies*, 32(5), 1754-1797.

19. Cong, L. W., He, Z., Li, J. (2018). Decentralized Mining in Centralized Pools. Retrieved from http://www.law.nyu.edu/sites/default/files/upload_documents/SSRN-id3160046_1.pdf.

20. Corallo, M. (2019, June 24). *Mining: No Good, The Bad, and The Ugly* [Video file]. Retrieved from https://www.youtube.com/watch?v=k_z-FBAil6k.

21. Dale, B. (2019, September 19). Everyone's Worst Fears About EOS Are Proving True. *Coindesk*. Retrieved from https://www.coindesk.com/everyones-worst-fears-about-eos-are-proving-true.

22. Dingman, W., Cohen, A., Ferrara, N., Lynch, A., Jasinski, P., Black, P. E., Deng L. (2019). Defects and Vulnerabilities in Smart Contracts, a Classification using the NIST Bugs Framework. *International Journal of Networked and Distributed Computing*, 7(3), 121-132.

23. Dujmovic, J. (October 15, 2018). The good and the bad of Tim Berners-Lee's new project on data privacy. *MarketWatch*. Retrieved from https://www.marketwatch.com/story/the-good-and-the-bad-of-tim-berners-lees-new-project-on-data-privacy-2018-10-12.

24. Eichholz, L. (2017, Aug. 25). *Private Blockchains!=Intranets*. Retrieved from https://medium.com/@liesleichholz/private-blockchains-intranets-eeb8066240af.

25. European Commission (2019). *Blockchain Now And Tomorrow.* Retrieved from https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-now-and-tomorrow.

26. Federal Trade Commissino (FTC). (2010, August 4). FTC Settles Charges of Anticompetitive Conduct Against Intel. *Press Release*. Retrieved from http://www.ftc.gov/news-events/press-releases/2010/08/ftc-settles-charges-anticompetitive-conduct-against-intel.

27. Federal Trade Commission (FTC). (2010, August 4). FTC Settles Charges of Anticompetitive Conduct Against Intel. *Press Release*. Retrieved from http://www.ftc.gov/news-events/press-releases/2010/08/ftc-settles-charges-anticompetitive-conduct-against-intel.

28. Fehér, K. (2019). Digital identity and the online self: Footprint strategies – An exploratory and comparative research study. *Journal of Information Science*, 1. Retrieved from https://journals.sagepub.com/doi/10.1177/0165551519879702.

29. Finney, B. (2018). *Blockchain and Antitrust: New Tech Meets Old Regs*, 19 *Transactions: The Tennessee Journal of Bussiness Law*, 19. 709-736.

30. Frankel, A. (2020, March 25). SEC wins injunction against Telegram blockchain launch in key ICO case. *Reuters*. Retrieved from https://www.reuters.com/article/legal-us-otc-telegram/sec-wins-injunction-against-telegram-blockchain-launch-in-key-ico-case-idUSKBN21C3N0.

31. Günther, S. (2018, June 1). Lisk—the mafia blockchain [Blog Post]. Retrieved from https://medium.com/coinmonks/lisk-the-mafia-blockchain-47248915ae2f.

32. Halpin H. (2017). *The Crisis of Standardizing DRM: The Case of W3C Encrypted Media Extensions*. Retrieved from. https://hal.inria.fr/hal-01673296/document.

33. Hassani, H., Huang, X. & Silva, E. S. (2019). *Fusing Big Data, Blockchain and Cryptocurrency*. Nature Switzeland, AG: Springer.

34. Hern, A. (2013, October 3). Bitcoin price plummets after Silk Road closure. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2013/oct/03/bitcoin-price-silk-road-ulbricht-value.

35. Hicks, S.R. (1935). Annual Survey of Economic Theory: The Theory of Monopoly. *Econometrica*, 3. 1-8.

36. Hyperledger. *Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric*. Retrieved from https://www.hyperledger.org/learn/publications/walmart-case-study.

37. Jacobs, R. (2018, February 12). The Good and Bad of Blockchain. *Chicago Booth Review*. Retrieved from http://review.chicagobooth.edu/finance/2018/article/good-and-bad-blockchain.

38. Kolber, A. J. (2018), Not-So-Smart Blockchain Contracts and Artificial Responsibility. *Stanford Technology Law Review*, 21 (2), 198-234.

39. Lee, T. B. (n.d.). *Frequently Asked Questions*. Retrieved from http://www.w3.org/People/Berners-Lee/FAQ.html (last visited Nov. 19, 2015).

40. Leising, M. (2017, June 13). Ether thief remains mystery year after $55 million heist. *Blomberg News*. Retrieved from https://www.bloomberg.com/features/2017-the-ether-thief/.

41. Lianos I. (2018). *Blockchain Competition*. Retrieved from https://www.ucl.ac.uk/cles/sites/cles/files/cles_8-2018.pdf.

42. Licklider, J.C.R. & Taylor, R. (1968). *The Computer as a Communication Device.* Retrieved from https://www.ais.org/~jrh/licklider/computer-as-communications-device.html.

43. Lopatka, J. E. (2000). United States v. IBM: A Monument of Arrogance. *Antitrust Law Journal*, 68 (1). 145-162.

44. Massarotto, G. (2016). Open Source Paradigm: Beyond the Solution to the Software Patentability Debate. *John Marshall Review of Intellectual Property Law, 15*, 647-675.

45. Massarotto, G. (2018). From Standard Oil to Google: How the Role of Antitrust Has Changed. *World Competition, 41* (3), 395-418.

46.

47. Massarotto, G. (2019a). *Antitrust Settlements: How a Simple Agreement Can Drive the Economy* (1st ed.). Wolters Kluwer.

48. Massarotto, G. (2019b). *From Digital to Blockchain Markets: What Role for Antitrust and Regulation*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3323420.

49. Massarotto, G. (2020a). Antitrust in the Blockchain Era. *Notre Dame Journal of Emerging Technologies* 2 (1) 253-279.

50. Massarotto, G. (2020b, May 19). Can Blockchain Be the Key to Compete in Today's Digital Era? [Kluwer Competition Law Blog Post]. Retrieved from http://competitionlawblog.kluwercompetitionlaw.com/2020/05/19/can-blockchain-be-the-key-to-compete-in-todays-digital-economy/?doing_wp_cron=1589904976.2744710445404052734375 .

51. Massarotto, G. (2020c, Feb. 24). Grasping the Meaning of Big-Tech Antitrust Consent. *Competition Policy International*. Retrieved from https://www.competitionpolicyinternational.com/grasping-the-meaning-of-big-tech-antitrust-consent/.

52. Massarotto, G. (2020d, Aug. 19). Is Blockchain the Real Antitrust Game-Changer? *Competition Policy International*. Retrieved from https://www.competitionpolicyinternational.com/is-blockchain-the-real-antitrust-game-changer/

53. May, T. C. (1988). The Crypto Anarchist Manifesto. Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html.

54. May, T. C. (1994). Crypto Anarchy and Virtual Communities. Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-virtual-comm.html.

55. Medium, Cryptocurrency. (2019, May 2). How decentralized is Cardano? [Blog Post]. Retrieved from https://medium.com/@undersearcher/how-decentralized-is-cardano-d3a47f985ce1.

56. Microsoft. *Confidential Consortium Framework*. Retrieved from https://www.microsoft.com/en-us/research/project/confidential-consortium-framework/.

57. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System 3, https://bitcoin.org/bitcoin.pdf.

58. Nikolaus Thumm & Garry Gabison, 2016. Patent Assertion Entities in Europe: Their impact on innovation and knowledge transfer in ICT markets. JRC Working Papers JRC103321. Retrieved from https://ideas.repec.org/p/ipt/iptwpa/jrc103321.html.

59. Orcutt, M. (2018, April 25). How Secure is Blockchain Really?. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/.

60. Organisation for Economic Co-operation and Development (OECD). (2018, November 28). *Personalized Pricing in the Digital Era*. Retrieved from http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP(2018)13&docLanguage=En.

61. Organisation for Economic Co-operation and Development (OECD). November 28, 2018. *Personalized Pricing in the Digital Era*. Retrieved from http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP(2018)13&docLanguage=En.

62. Ou, E. (2017). A hundred of Years of Crypto Anarchy. Retrieved from https://elaineou.com/2017/08/03/a-hundred-years-of-crypto-anarchy/.

63. Planet Compliance. (2020, May 11). *Innovation & Regulation in Finance*. Retrieved from https://www.planetcompliance.com/2017/05/10/top-10-scandals-rocked-blockchain-world/.

64. Poon, J. & Dryja, T. (2016), *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. Retrieved from http://lightning.network/lightning-network-paper.pdf.

65. Popper, N. & Isaac, M. (April 16, 2020). Facebook-Backed Libra Cryptocurrency Project Is Scaled Back. New York Times. Retrieved from https://www.nytimes.com/2020/04/16/technology/facebook-libra-cryptocurrency.html.

,

66. PricewaterhouseCoopers (PwC) & Crypto Valley (Mar. 2019). 4th ICO/STO Report. Retrieved from https://cryptovalley.swiss/wp-content/uploads/ch-20190308-strategyand-ico-sto-report-q1-2019.pdf.

67. Puthal, D., Malik, N., Mohanty, S. P., Kougianos E. & Yang, C. (2018). The Blockchain as a Decentralized Security Framework. *IEEE Consumer Electronics Magazine*, *7*(2), 18-21.

68. R3. Retrieved June 3, 2020, from https://www.r3.com/.

69. Ren L. & Ward, P. A.S. (2019). Pooled Mining is Driving Blockchains Toward Centralized Systems. *IEE*.

70. Schneier, B. (2019b).“Click Here to Kill Everybody” Talks at Google [Video file]. Retrevied from https://www.youtube.com/watch?v=GkJCI3_jbtg.

71. Schneir, B. (2019a, January 22). Keynote: Security, Trust, and Blockchain-Bruce Schneier [Video file]. Retrieved from https://www.linuxfoundation.org/blog/2019/01/how-blockchain-changes-the-nature-of-trust/.

72. Shein, E. (January 22, 2019). *How Blockchain Changes the Nature of Trust*. Retrieved from https://www.linuxfoundation.org/blog/2019/01/how-blockchain-changes-the-nature-of-trust/.

73. Shilov, K., (2019, July 12). Programmable Ownership: What Security Tokens mean for Individuals. *Hackernoon*. Retrieved from https://medium.com/hackernoon/programmable-ownership-what-security-tokens-mean-for-individuals-d18a7f56e088.

74. Sidak,G. J. (2013). The Meaning of FRAND. *Journal of Competition Law & Economics*. 9(4). 931-1055.

75. Statista (2020). *Number of monthly active Facebook users worldwide as of 1st quarter 2020*. Retrieved from https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

76. Statista (2020b). *Worldwide desktop market share of leading search engines from January 2010 to January 2020*. Retrieved from https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/.

77. Stylianou, K. (Apr. 26, 2019), *What can the First Blockchain Antitrust Case Teach us about the Crypto-Economy?*, Retrieved from https://jolt.law.harvard.edu/digest/what-can-the-first-blockchain-antitrust-case-teach-us-about-the-crypto-economy.

78. Submarine Cable Networks. *Curie*. Retrieved from June 1, 2020 https://www.submarinenetworks.com/en/systems/brazil-us/curie.

79. Sung, H. C. (2018). When Open Source Software Encounters Patents: Blockchain as an Example to Explore the Dilemma and Solutions, *J. Marshall Rev. Intell. Prop. L.,* 18, 55-82.

80. Szabo, N. (2017, February 9). Enumerated [Blog Post]. Retrieved from http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html.

81. Tapscott, D. & Tapscott, A. (2016), *Blockchain Revolution*. *How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. Peguin Random House.

82. Tasca, P. & Tessone, C. J. (2019) A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. *Ledger*, *4*. https://doi.org/10.5195/ledger.2019.140.

83. Tuwiner, J. (2020 March 12). Bitcoin Mining Pools. *Buy Bitcoin Worldwide*. Retrivied from https://www.buybitcoinworldwide.com/mining/pools/.

84. UCL CBT (2019). *DLT in the Supply Chain Report*. Retrieved from http://blockchain.cs.ucl.ac.uk/dlt-in-the-supply-chain-report/.

85. UCL CBT (2019). DLT on Supply Chain. Retrieved from http://blockchain.cs.ucl.ac.uk/dlt-in-the-supply-chain-report/.

86. United American Corp. v. Bitmain, Inc. 2018 1:2018cv25106 (D.C. Flo.).

87. Webach, K. (2018). *The Blockchain and the New Architecture of Trust* (1st ed.). MIT Press.

88. Webfoundation (n.d.). *History of the Web*. Retrieved from https://webfoundation.org/about/vision/history-of-the-web/.

89. Werbach K. & Cornell N. (2019), Contracts Ex Machina. *Duke Law Journal. 67*, 313-382

90. *What is Bitcoin's Lightning Network?* (2018, February 23). *Coindesk* Retrieved from https://www.coindesk.com/learn/bitcoin-101/what-is-the-lightning-network.

91. Wright, A. & De Filippi, P. (2018). *Blockchain and the Law. The Rule of Code* (1st ed.). Harvard Univ. Press.

92. Xu, X., Weber, I. & Staples, M. (2019). *Architecture for Blockchain Applications*. Nature Switzeland, AG: Springer.

93. Yu, P. K. (2007). *Intellectual Property and Information Wealth: Issues and Practices in the Digital Age*. Westport, Connecticut London: Praeger.

94. Zak P. Z. (2017). The Neuroscience of Trust. *Harvard Business Review*. Retrieved from https://hbr.org/2017/01/the-neuroscience-of-trust.