LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Department of Business and Management

Bachelor's Degree in Management and Computer Science

Course of Business Law and ICT

Blockchain and Smart Contracts: the EU's (lacking) view

SUPERVISOR:
Prof. Andrea Giannaccari

CANDIDATE:
Luca Agostini
(238401)

ACADEMIC YEAR 2020/2021

Table of Contents

INTRODUCTION

More than a decade has passed since the launch of the first cryptocurrency in history. It was the year 2009 when the "famous" (but still unknown) Satoshi Nakamoto created Bitcoin, the currently most used and popular electronic money in the world. The same world that, day after day, is taking on an increasingly evident digital drift, which (especially during this pandemic period) seems to be necessary. For this reason, in my dissertation, I decided to deal with a “hot-topic” as interesting and hyped as, at the same time, discussed and criticized today: the blockchain technology. Specifically, we will see how (and if) this type of tech, along with smart contracts, is regulated within the European Union.

The first chapter has a purely introductory purpose, trying to explain to the reader in a quick but clear way the fundamental principles of blockchain and smart contracts. What are they? How do they work? Which are their advantages and disadvantages? These are the main questions that we will try to answer in a (hopefully) detailed and exhaustive manner. A short paragraph, at the end of the chapter, will briefly summarize the key properties above.

In the second chapter, the legal aspects (as well as the legal issues) related to blockchain and smart contracts in the EU will be studied. The digitization process is constantly evolving, and it often proves to be much faster than the law itself. Given its decentralized nature, can the blockchain comply with the current European legal framework? In particular, GDPR and Antitrust law are at the center of the debate.

Across the third and final chapter, after a little premise, we will try to outline the digital future of Europe, through the analysis of a new blockchain-based governance. To this aim, we will take a closer look at the case of Malta, the American example of the state of Wyoming, and the recent proposals of the European Union in this respect. At the moment of writing, the only certainty seems to be the uncertainty concerning the regulation of the blockchain technology, particularly in the EU’s context.

CHAPTER 1 - The Blockchain Technology and the Role of Smart Contracts

1.1. What is a Blockchain?

1.1.1. A Quick Overview

A blockchain, in a broad sense, is a Distributed Ledger Technology (DLT)[1] which records all the transactions that occur inside a peer-to-peer network[2]. The main feature of a blockchain is that it allows untrusted participants (called "nodes") to communicate among each other in a secure manner, and without the need of a trusted third party (like a bank), thanks to a decentralized database system. Specifically, a blockchain is a sorted list of blocks, each of which is identified by a cryptographic hash function[3]. Every block references the previous one, resulting then in a chain of blocks. Any block consists of a set of transactions, which cannot be changed. This is in order to guarantee the integrity of the transactions and for preventing the so called "double-spending problem"[4].

As the first generation of blockchain technology, there is the invention of cryptocurrencies. Which are digital (or electronic) currencies based on cryptographic techniques and a peer-to-peer network. They are, of course, different from fiat currencies[5]. The first and most popular example of cryptocurrency is bitcoin (BTC). An electronic payment system created in 2008 by a person (or a group of people) whose identity is still unknown, using the name Satoshi Nakamoto. Bitcoin allows two untrusted parties to safely transact digital money with each other, through the SHA-256 algorithm[6]. All the transactions are verified by special nodes called "miners"[7], who generate a new

[1] A Distributed Ledger Technology (DLT) is a protocol that enables the functioning of a decentralized digital database.

[2] A peer-to-peer (P2P) network consists of a set of computers connected together, with equal permissions for processing data.

[3] A cryptographic hash function is an algorithm that takes an arbitrary amount of data input and produces a certain (fixed) output of encrypted text, called "hash value".

[4] The double-spending problem is, basically, the risk that a digital currency can be spent twice.

[5] Fiat currencies are any money declared as legal tender by governments (like the euro or the US dollar).

[6] The so-called "Secure Hash Algorithm 256" (or, simply, SHA 256) is a mathematical process which produces a 256-bit (64-character long) random sequence of letters and numbers out of any input. It is considered as one of the safest ways to protect digital information.

[7] Miners are the ones who develop the activity of "mining": the process of adding transactions to the blockchain.

block of transactions after solving an advanced mathematical puzzle called "Proof of Work" (PoW)[8]; which is essentially used to determine how the blockchain achieves consensus. For this reason, along with "Proof of Stake" (PoS)[9], PoW is called "consensus mechanism". Both PoW and PoS are the current requirements to check the validity of the transactions which take place on a blockchain.

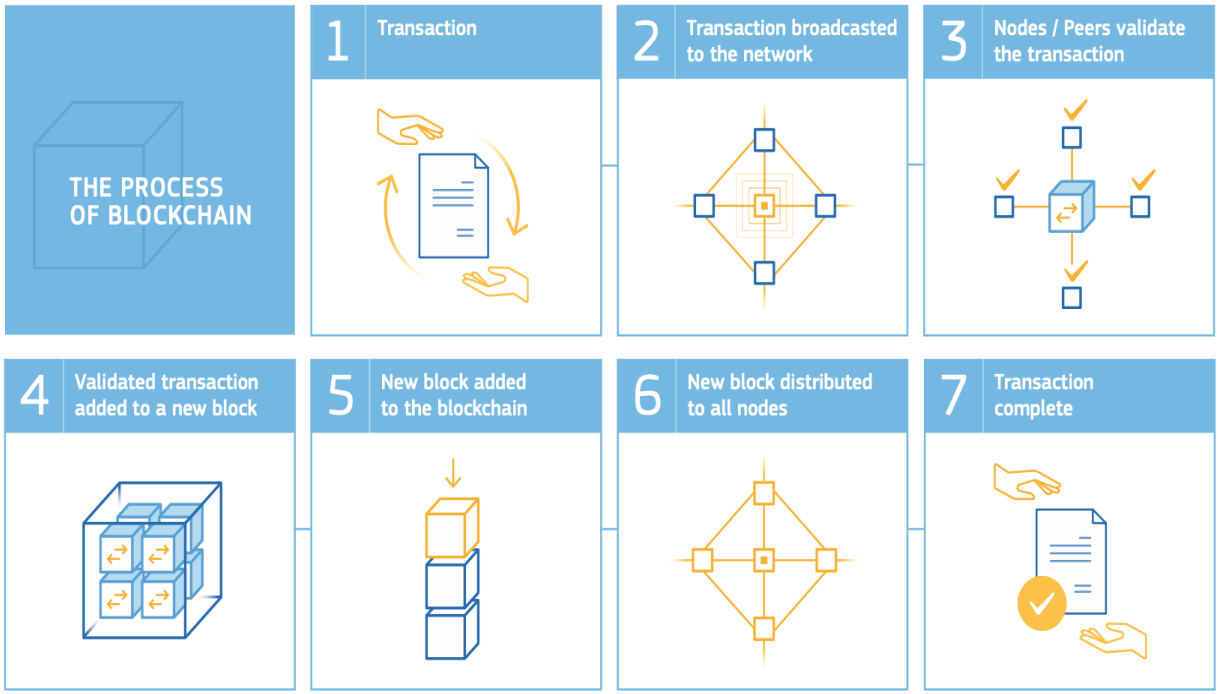

Figure 1: "THE PROCESS OF BLOCKCHAIN"

Source: Blockchain now and tomorrow: assessing multidimensional impacts of distributed ledger technologies (EU Science Hub – 2019)

Therefore, the blockchain is considered a revolutionary technology because it reduces risk and helps businesses in various ways. It is not only about Bitcoin and cryptocurrencies. Thanks to its ability to generate fairness, indeed, this technology is impacting a variety of sectors that goes, for instance, from voting mechanism and cross-border payment to real-time IoT (Internet of Things) operating system and NFT[10] marketplaces.

[8] Proof of Work (PoW) is a form of cryptographic proof in which one party proves to others that a certain amount of computational effort has been expended for some purposes.

[9] Proof of Stake (PoS) is a blockchain protocol that work by selecting validators in proportion to their stake in the associated cryptocurrency.

[10] "Non-Fungible Tokens" (NFTs) are blockchain cryptographic tokens which are unique and cannot be replicated.

There are two types of blockchain. Namely, public (or permissionless) and private (or permissioned) blockchains. In a public one, every anonymous user can join the network, read the content and send a new transaction or verify the correctness of the blocks. Some examples of public blockchains are Bitcoin, Litecoin and Ethereum. In a private one, instead, only users with permission can join the network, make or send transactions to the blockchain. Some examples of private blockchains are Everledger, Hyperledger and Quorum.

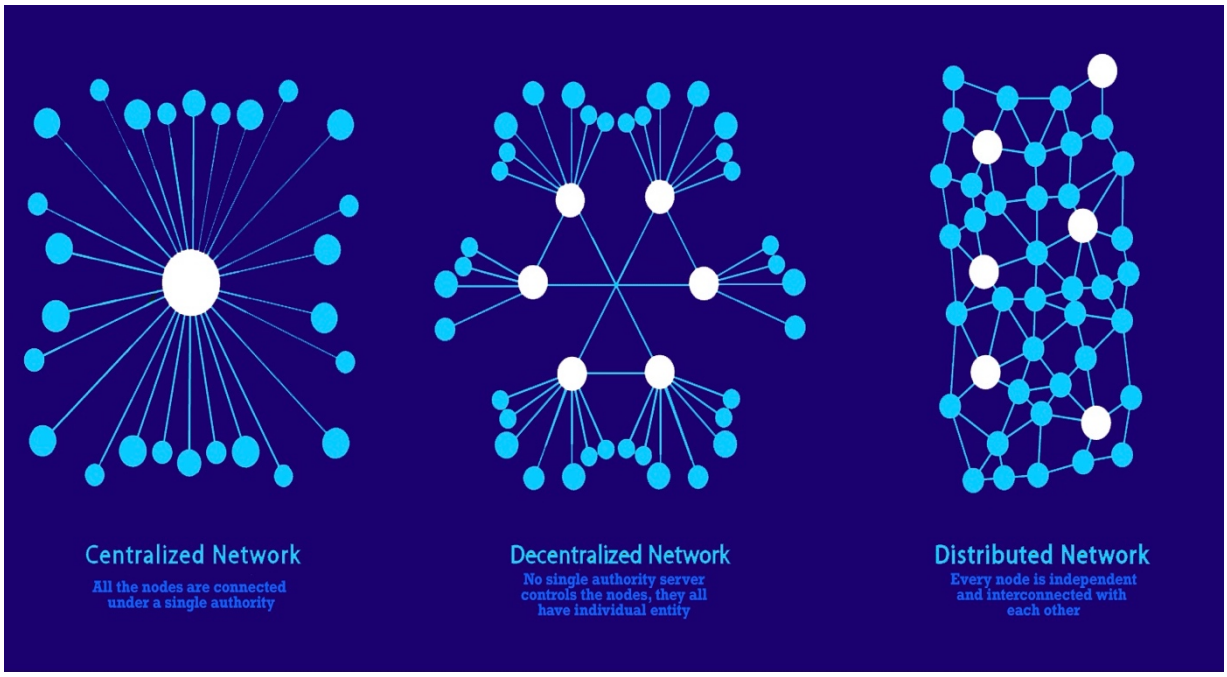

Figure 2: "Centralized vs Decentralized vs Distributed Network: An Overview"
Source: https://blockchainengineer.com/centralized-vs-decentralized-vs-distributed-network/

1.1.2. Key Properties

There are several advantageous properties related to the blockchain technology. The first one is immutability. A blockchain cannot be changed. It will always remain an unalterable network. Rather than relying on centralized authorities, it is run by the people who use it. Moreover, every node owns a copy of the digital ledger and, in order to add a transaction, each of them needs to check its validity. This promotes transparency, making the blockchain corruption-proof.

Blockchain can also grant enhanced security. Thanks to cryptography, it offers much safety with respect to other techs. It uses cryptography to ensure that all the data in the blocks is kept secure from unauthorized access. Since any kind of information is hashed cryptographically, the information on the network hides the true nature of the data. All the blocks in the ledger come with a unique hash,

containing the hash of the previous one. This means that, for tampering data, one has to change all the hash IDs (something that is virtually impossible). We will have a private key to access the data and a public one to make transactions.

Blockchain offers a faster settlement compared to traditional banking systems as well. Thus, users can transfer money (relatively) faster. Another fundamental fact is represented by smart contract systems, which let users make faster deals among each other. Furthermore, without the presence of an intermediary, people can transfer money with a minimal fee.

Figure 3: "Blockchain Benefits – Column List"
Source: https://blog.infodiagram.com/2019/02/explain-blockchain-technology-by-diagrams-ppt.html

1.1.3. Main Challenges: beyond the hype

As a result, the potential benefits of the blockchain have rapidly grown the enterprises' interest in the prospect that DLTs could improve business efficiency. However, for all of the possible features that this technology promises to realize, we currently see little in terms of real-world practical deployment. There are still significant challenges to the broad adoption of blockchain technologies. Actually, according to some people, blockchain seems to be over-hyped and, unless someone can invent a real "killer application" for it, it will not evolve into the disruptive technology that some people were hoping for.

First of all, the blockchain's performance and scalability are limited. Though many advances have already been incorporated into lots of programs, most blockchains are complex. This complexity poses a barrier to the technology's progress. Bitcoin, for instance, is able to process between seven and ten transactions per second. Visa network, based upon a centralized model, can process an estimated 24,000 transaction messages per second. This is due to the fact that there is a restricted space for transactions in the blockchain. Besides, just like other similar cryptocurrencies, bitcoin uses weighty energy resources.

Yet, there are concerns about privacy. Some stakeholders, particularly in the law enforcement and regulatory sectors, are worried that the blockchain-based records obscure the identity of actors. Others believe that privacy protection is not strong enough, since the first distributed ledgers were designed with transparency in mind, allowing all participants to view every transaction. Even if Bitcoin and other blockchains have generally been resistant to hacks, with the integrity of their ledgers preserved, there have been numerous reports of hacks within the crypto ecosystem.

Furthermore, there are challenges concerning the interoperability of the blockchain applications. The success of most use cases will depend on linking in some way databases to legacy infrastructures. The objective is to enable decentralized mechanisms for asset transfers in these situations. Although potentially reachable, there is a great deal of work needed to attain such movements of data and applications amongst new DLTs and existing architectures. The solutions aimed at improving the scalability blockchain's processing capacity may also be extended to accomplish interoperability across blockchains.

There are even trade-offs concerning the governance of blockchain. One of the features of blockchains is that there must be a consensus across a distributed network, for which there is no controlling entity. And this, for some software updates, can be hard to fulfill. When a full consensus has not formed, several blockchains have experienced chain divisions. And this leads to what is called a "hard fork"[11].

Ultimately, most of the real-world usage so far has been related to cryptocurrency speculations. Many established companies are engaging in pilots and proofs of concept regarding how to use blockchain technology, but actually very few has (as of now) transitioned to relying on a blockchain. Hence,

[11] A hard fork is a radical change to a network's protocol that makes previously invalid blocks and transactions valid, or vice-versa.

blockchains need to be more fully brought within public policy and legal frameworks. Only with clear rules will there be broad adoption of blockchain technologies, along with their potential to transform the industry.

1.2. What are Smart Contracts?

1.2.1. A Quick Overview

Smart contracts are computerized transaction protocols that automatically execute or control the terms of an agreement. In particular, they are executable code (run on a blockchain) aimed at easing and enforcing the conditions of an arrangement. A smart contract, then, assures lower transaction fees than typical systems which require a trusted third party (a middleman).

```
template FixedSupplyTokenProposal
    with
        owner: Party
        issuer: Party
        amount: Decimal
    where
        signatory issuer -- Issuer creates proposal

    controller owner can -- Proposed owner can choose to accept
        Accept : ContractId FixedSupplyToken
            do create FixedSupplyToken with owner, issuer, amount -- Which creates the token

template FixedSupplyToken
    with
        owner: Party
        issuer: Party
        amount: Decimal
    where
        Signatory issuer, owner
```

Figure 4: "Smart Contract Example Code"
Source: https://daml.com/blog/engineering/the-world-of-smart-contracts-using-daml-solidity/

The idea of smart contracts came for the very first time from Nick Szabo (a popular computer scientist, legal scholar and cryptographer) in 1994, but it did not see the light until the advent of the blockchain. A smart contract can also be thought of as a system which releases digital assets to the involved parties (once predetermined rules have been met). For example, Alice sends X currency units to Bob, if she receives Y currency units from Carl. Several distinct definitions of smart contracts have been discussed in the literature. We will classify all of them into two leading categories, namely:

"smart contract code" (whose capability utterly depends on the blockchain, and the programming language used) and "smart legal contract" (whose capability depends, instead, on political and business institutions). While smart contract code is intended as code stored, verified and executed on a blockchain, smart legal contracts are code that completes or substitutes traditional legal contracts.

Smart contracts have some features in common. Since they exist on the blockchain, they have a state (like RAM in a pc), which is shared across the whole network. Each node that runs on a blockchain has a copy of the smart contract's state, which cannot be altered. Although there are ways to extend or replace some parts, there is no way to manipulate their content without drawing the attention of the network. The logic of a smart contract cannot be distorted and there is no room for interpretation. They exactly act like a deal between two parties, with one of which needs no judge, since the output is produced from the input deterministically. Additionally, smart contracts gave us the opportunity to create any kind of token without having to launch a new blockchain. With Ethereum, for example, a token become just a piece of code with specific functions. A smart contract might be programmed to release payments, or it may be used to enforce rights for digital assets' holders. Some of these ideas will be explored in a later section of this paper, covering the main applications of smart contracts.

They work by following simple conditional statements[12], written into code on a blockchain. Once certain conditions are verified, a network of computers executes the actions. These actions could range from releasing funds to the appropriate parties to issuing a ticket. When the transaction is completed, the blockchain is then updated. That means transactions cannot be changed, and only contractual parties can see the results. In a smart contract there can be as many stipulations as needed to satisfy the participants. In order to establish the terms of a smart contract, nodes must determine how transactions are represented on the blockchain, agree on the rules that govern the transactions to be carried out and define a framework for solving potential disputes. Finally, smart contracts can be programmed by developers, organizations, web interfaces, and many other online tools.

[12] Conditional statements are used to perform different actions based on different conditions. They allow a computer program to make decisions based on the given conditions.

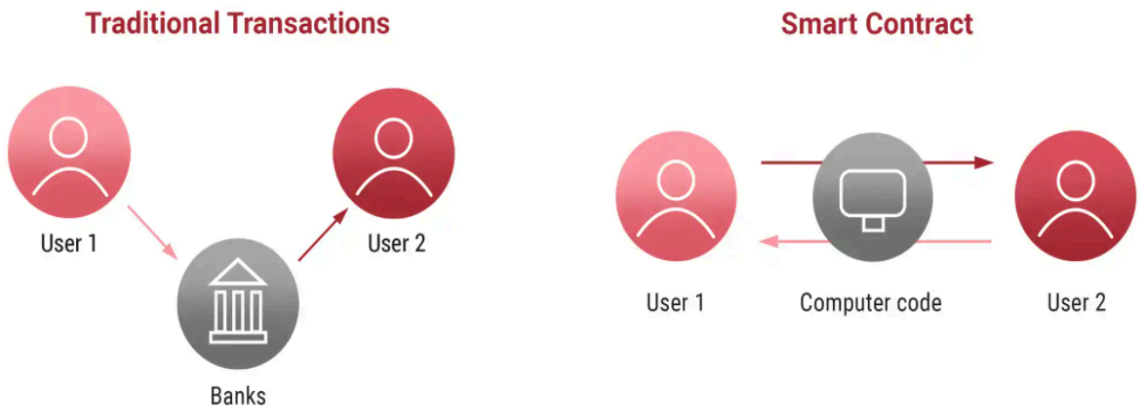

Figure 5: "How Smart Contracts Work?"
Source: https://www.ulam.io/blog/smart-contract-definition-use-cases/

1.2.2. Ethereum Platform & Practical Applications

Smart contracts can be developed in different blockchain-based platforms. Many of them offer distinctive features and support high-level programming languages for deploying smart contracts. The most important and popular one is, undoubtedly, Ethereum. While most people know Ethereum thanks to its token (Ethereum, Ether or ERC-20), many might not be aware of that it is the world's leading smart contract platform, and the best choice for several developers. Ethereum is a smart contract ecosystem created by Vitalik Buterin and other co-founders in 2013. It is a Proof of Work blockchain network hosting the Ethereum Virtual Machine (EVM), which is a "Turing-complete system"[13]. The Ethereum platform is also a hotspot for some "DeFi" (Decentralized Finance) applications.

A key benefit of this platform is the degree of standardization and the support offered. Once a set of clear guidelines for developers was published, Ethereum have made smart contract development easier and less risky. Moreover, apart from having the biggest market capitalization among all the smart contract platforms, Ethereum is completely dedicated to improving the way smart contracts are created and run. There are distinct practical applications where smart contracts can be applied.

[13] A system can be considered to be "Turing-complete" if and only if can be used to simulate a Turing machine. Almost all programming languages are Turing-complete today. The concept is named from the famous English mathematician and computer scientist Alan Turing.

Amongst others:

- Internet of Things and Smart Property

There are billions of nodes sharing data among each other through the Internet. Smart contracts can allow those nodes to share or access digital properties without a trusted third party.

- Music rights management

A possible use case is to record the music's ownership rights. A smart contract can enforce payments for music owners if a song is used for commercial purposes. It also ensures that those payments are being distributed between the music's owners.

- E-commerce

Another potential use case is to facilitate the trade between untrusted parties, without the need for a middleman. This would result in a reduction of the trading costs. Smart contracts can release the payment to the seller, once the buyer is satisfied with the good or service (s)he received.

- Insurance

Smart contracts can offer advantages in speeding up the claims of insurance's processes. An example could be the life insurance. Their policy terms would be encoded into a smart contract. In case of passing away, the death certificate would be provided as the input trigger for the smart contract in order to release the payment to the named beneficiaries.

- Supply Chain and Logistics

The use of smart contracts is revolutionizing the supply chain and logistics sector as well. Blockchain can provide a permanent record of the transit of goods among multiple handlers. Payments can be executed automatically upon the receipt of delivery, and inventory levels automatically updated in real-time.

- Rights for Digital Token Holders

Asset tokenization may mean individual token-holders have rights. These rights can be, here again, coded into a smart contract. If firm's stocks are tokenized, shareholders have voting rights. And, through smart contracts, the person's voting right is granted when every ballot is opened up. They also allow people to cast their vote and to vote from remote.

1.2.3. Pros & Cons

Smart contracts have the substantial potential to bring radical changes in the way international business are executed by speeding up transactions, reducing paperwork and causing cost-efficiency. On the other hand, there also exist some drawbacks in developing smart contracts.

Starting from the positive features, we can highlight:

- Disintermediation: through which contractual parties can enter into agreements with no dependence on a middleman.
- Efficiency, Accuracy and Rapidity: once a condition is met, the contract is automatically executed. Since smart contracts are digital and automated, there is no paperwork to process, and no time spent finding errors manually.
- Trust and Transparency: without a third party involved, and since encrypted transaction records are shared across the nodes, there is no need to question whether information has been altered on purpose for personal reasons.
- Security: since blockchain transaction records are encrypted, they are very hard to hack. Hackers would have to alter the entire chain to change a single record, because each record is connected to the previous and the following ones on a distributed ledger.

As to the risks:

- Confidentiality: although enterprises desire transparency, they hesitate to use a blockchain and to put their contractual information on it. Ethereum does not have an option for private smart contracts. Therefore, businesses will have to select their blockchain platform based on their needs.
- Accuracy: since a smart contract is a computer program, each term and condition of the contract needs to be coded, and there is possibility of misinterpretation or omission by the programmer. The more we use smart contracts, the more we could encounter loopholes in the code.
- Unreliable Inputs: for traditional contracts, the parties can proceed to a judicial court for redressal. But this is not possible with smart contracts, where legal validity is still largely debated.

- Bugs in the Code: they could lead to disputes and procedural complications concerning the identification of errors, and the parties responsible for those. There could be unforeseen repercussions.

1.3. Summing Up

Let us conclude this first introductory chapter summarizing the most important notions concerning the blockchain technology and the smart contracts.

A blockchain is a Distributed Ledger Technology (DLT) which, through a decentralized database system, allows its peer-to-peer network's participants (also known as "nodes") to make transactions among each other in a very safe way, and without a trusted third party. Specifically, it is a technology based on cryptography and strictly related to the invention of cryptocurrencies, whose main example is surely bitcoin (BTC). In order for them to reach consensus, the circulation of these digital (or electronic) currencies is granted thanks to the so-called "SHA-256" algorithm. Transactions are verified by "miners", who must solve a mathematical puzzle called "Proof of Work" (PoW) for generating new blocks. There are two kinds of blockchain technologies: public (or permissionless), in which anonymous users can operate across the network; and private (or permissioned), in which only users with permission can operate across the network. The key features of a blockchain are transparency, fairness, immutability, enhanced security and faster settlement. Therefore, since it reduces risks and can help corporations, we can say that this technology is revolutionary. Nevertheless, there are also concerns about it. Performance and scalability of blockchains are still limited, and challenges regarding privacy or interoperability have arisen as well. Not to mention the huge energy consumption of the bitcoin. For this reason, according to some people, blockchain is an overrated tech. We will see then whether it will be just a matter of hype.

Smart contracts are, essentially, digital contracts automatically executed on a blockchain technology. In particular, they are executable code run on a blockchain platform (like "Ethereum") for facilitating and enforcing the terms of an agreement in a simple way, without the need for an intermediary. We can divide them into two main categories: "smart contracts code" (which are intended as code stored and verified on a blockchain) and "smart legal contracts" (which are intended as code for completing or substituting traditional legal contracts). There are several practical applications where smart contracts can be applied. Amongst others, we can list: IoT, E-commerce, insurance and supply chain. Their key properties are disintermediation, efficiency, rapidity, transparency and security. On the

other hand, accuracy and confidentiality issues have to be underlined. Businesses still hesitate to rely on blockchain technologies and to put their contractual information on it. Additionally, since a smart contract (whose legality is still discussed) is a computer program and each condition needs to be coded, there is possibility of misinterpretation or even omission by the programmer with consequent unpredictable repercussions.

CHAPTER 2 - From the Current European Legal Perspective

2.1. The Legal Issues of Blockchain & The Legality of Smart Contracts

As of today, in order to enable blockchain markets to raise, both businesses and lawmakers must collaborate together for creating new engagement rules. Regulators and policymakers should yield clear guidelines and set basic principles to attract investors, ensure costumer protection and guarantee citizens' rights. One of the main issues is doubtless related to competitive practices and fair competition within the European law, of which we will discuss in detail in the last paragraph of this chapter dealing with the antitrust law (regulations which encourage and promote competition among corporations). A blockchain-based network should enhance efficiency and lower boundaries for new competitors to access digital marketplaces. To this aim, let us have a deeper understanding of three main topics to be taken into account. Particularly, in terms of:

- Legal value of Blockchains as Registries

A transaction to be legalized requires legal recognition of the digital signatures, timestamps, validations and certain documents. In Europe, these requirements are regulated by eIDAS (electronic IDentification, Authentication and Trust Services regulation), that recognizes three different levels of digital signatures: simple, advanced and qualified. Blockchain technology can only meet the criteria for the first two but, to be legally binding, it would need to meet also the highest level (qualified) which uses a recognized Trust Service Provider (TSP). This is the reason why transactions made on a blockchain-based platform do not have legal authority by themselves.

- Territoriality

Determining in which country damages occur is complicated, so we may need to revisit some aspects of the current European private international law. To reach a decent jurisdictional harmonization among all the Member States, we might adopt a new approach to develop already existing legal tools. Regulators have to cooperate across national borders for integrating the distinct legal remiges and cope with risks, like market manipulation and potential monopolies.

- Liability

Two key aspects of liability should be then addressed: liability of core software developers and liability of network actors. As an open-source software, blockchain can be used to achieve both good

and bad objectives. Charging core software developers with responsibility for a potential unlawful usage of the program does not seem proper. Imposing responsibility on core software developers could lead some of them to anonymity. And this can also represent a difficulty in enforcing liability on the network's participants.

The act of transacting results in enforceable radical changes on the rights deriving from the specific asset considered. To exist in the real world, the assets transacted on a blockchain should be protected by rights. The European Union, indeed, is putting an effort for figuring out how to legalize blockchain and smart contracts. However, we are still behind with respect to America and Asia (for example); and regulators should increasingly find the right solution to support the advancement of this technologies.

Generally speaking, a contract is usually enforced by the parties. Only in case of disputes there is a need for enforcement, and this process costs effort. Therefore, in the modern society, the possibility to grant contracts' performance and completion ex ante is preferable. Since litigations can be resource-intensive, the ascent of "contractware" could be a great opportunity.

The instantiation of a contract does not have to be necessarily inside a hardware or in a physical piece of property, rather it could be in a piece of program. This leads us to consider (computer) code like law. Now, let us see how this process has been expanded during the recent times.

2.2. Rule of Code vs. Rule of Law: from "Code is Law" to "Law is Code"

Given the aforementioned features of the blockchain, the mainstream adoption of this technology may require a shift in the way we perceive the role of law. We might need to re-think the mechanisms we use to regulate individuals and society, in order to better grasp the emergence of this new set of technological rules.

Thanks to digital technology, code has been established as the dominant form for regulating the people's behavior on the Internet. Programs can enforce rules more efficiently than legal code, but there are several limitations as well. This is mainly because transposing the flexibility and the ambiguity of legal rules into a programming language interpreted by a machine is not an easy task. With the emergence of blockchain (along with smart contracts), code has assumed a stronger role in regulating the actions of the Internet users. Therefore, we have officially passed from the traditional notion of "code is law" (code having the effect of law) to the new conception of "law is code" (law defined as code). Law and tech can influence each other in many ways. They interact by means of a

complex system of dependencies and interdependencies. Through the progressive growth of ICT, their relationship has significantly evolved.

Over the Internet, regulations are done by private means within an environment that (due to its transnationality) seems to go beyond the jurisdiction of each state. The deployment of Internet network and the development of information technologies have generated a new status for humans, in which rules are set by software code. Software applications are different from hardware devices. Code can be produced using just a computer and can be easily distributed via any network connection, while building physical artefacts requires raw materials and production facilities. For this reason, the barriers to entry are much lower than in other contexts for software developers. This explains the exponential expansion of software applications in the past couple of decades.

Yet, as oppose to the physical world in which the costs of reproduction are often high, in the digital world it is virtually null. Even the cost of distributing information is close to zero. Moreover, since software code is (by nature) digital, it can be modified or replicated from everybody; and any piece of program can be reproduced all around the world regardless of national boundaries. Thus, it is difficult for a country to avoid or prevent the importation and exportation of computer code. However, every device manufacturer or online operator is subject to the laws of her/his nation by disclosure obligations and monitoring requirements.

The idea that "Code is Law" has now become a popular conception. Recently, there has been a tendency by both public institutions and private actors to replace current laws (which can only be enforced ex-post through state intervention) by technical regulations (which can be enforced ex ante through code). While it is true that code is increasingly assuming some of the typical functions of law, it is also true that law is progressively starting to assume the characteristics of code. To this end, blockchain technology reinforces the trend to rely on code rather than on law; especially for regulating transactions. Combined with smart contracts, a blockchain promotes a new way of thinking about law. As a result, legislators could draft contractual rules in a manner closer to the technical ones.

Blockchain is not only a neutral technology, but also a technical artefact with a specific architecture. Besides, since blockchains bypass the need for a central system and smart contracts can be executed and run on a distributed network, they are all transnational and reduce the risk of prosecution for legal proceedings. Latest discussions are focused on the optimization and efficiency of smart contracts. With respect to traditional contracts, their security level is superior and transaction costs are very low. Today, more and more interactions are mediated through technology, and we are delegating to tech the interpretation and application of law. But, as we increasingly rely on technological means for

enforcing legal rules, we face the risk that law progressively assume the characteristics of code. And, with the appearance of blockchain, this issue has become reality.

Code can be used for enforcing existing legal provisions and also for defining them. We are currently experiencing a radical change in the way we intend the law. Nevertheless, laws should not be entirely and exclusively defined through technological processes, as tech cannot replace the democratic debate which must take place in the legislative branch. The principal risk is that, while the legal system provides a series of policies and procedures for society to collectively agree upon certain rights or obligations and whose legitimacy can be put into question, technical rules can be unilaterally imposed by software developers. Furthermore, in the context of smart contracts, since their enforcement is done through the technological framework itself, it becomes possible for private parties to bypass the legal safeguards required by the law. Thus, once a smart contract is executed, it will be enforced regardless of whether or not it is qualified as a valid contract under the law.

Anyway, we cannot forget that blockchain-based applications are meant to operate in the real world, which is regulated by traditional rules of law. As to smart contracts, in order for them to be as effective as their typical counterparts, they must be actionable in the real world as well. Several legal rules are intended to be generic enough for being applicable to various situations. By definition, they must have a high level of abstraction for being able to encompass as many cases as possible. This is why legal rules need to be interpreted by a judge, and they have been drafted to and for humans. Therefore, in order to give meaning to the law, accounting for the initial intention of the legislator (along with human interpretation) is pivotal.

2.3. The Rise of "Lex Cryptographia"

The widespread deployment of the blockchain technology has led to a new subset of law, the so-called "Lex Cryptographia". In particular, it consists of a set of rules administered through self-executing smart contracts and decentralized autonomous organizations (DAOs)[14]. Since blockchains are becoming widely adopted, centralized systems and authorities could lose their ability to watch over the individuals' activities. As a result, there will be an increasing need to focus on how to regulate and shape the establishment of these emerging decentralized technologies.

[14] A "Decentralized Autonomous Organization" (DAO), sometimes called "Decentralized Autonomous Corporation" (DAC), is an organization represented by rules encoded as a computer program, which is controlled by the organization's members themselves.

Legal theory has always sought to harmonize the struggle among nations, markets and individuals; trying to find the right balance between the interests of the public sphere and those of the private one. With the abrupt advent of decentralized applications and autonomous agents, there is no doubt that the traditional conceptions of the Internet regulations have to be reviewed.

By means of an appropriate mix of these different levers of power, legal theorists have persuasively discussed that our use of the Internet could be tamed. Countries habitually approve laws in order to ban online services and for employing coercive power to shut down illegal services (like, for example, online gambling). Governments (along with private interests) progressively manipulate markets by pressuring search engines, advertising networks and other financial intermediaries. The emersion of Lex Cryptographia may oblige us to reevaluate the interactions between them.

Current technologies can be used to institute new rules for organizations and, potentially, for governmental entities. Automatically enforced through self-executing code, smart contracts might edit some of the basic principles of property law, effectively turning property rights into a subset of contract law. Judicial enforcement of law could also be displaced by blockchain technology, and smart contracts could be made to rely on a certain degree of human judgment during their execution. For instance, in order to determine whether or not predefined conditions have been met, contractual clauses could be made dependent on the judgment of one or more external parties (known as "Oracles"). One of these parties could be the judiciary, but it could be represented by independent arbitrators as well. Subsequently, these decentralized judiciaries can narrow the role of centralized judicial bodies.

As of now, the rise of Lex Cryptographia can offer people access to alternative currencies, global markets, automated and trustless transactions systems, self-enforcing smart contracts, smart property and cryptographically activated assets. Combined, all these elements could be used to promote individual freedoms and user autonomy. Hence, people could be granted equal access to basic digital institutions and infrastructure, regardless of their nationality. Through the experimentation of emergent blockchain-based applications, decentralized institutions and governance models could be designed and structured iteratively, rather than being imposed by centralized legal statutes. This aspect could significantly contribute to that disintermediation process which is characterizing the online environment.

In spite of the blockchains' benefits, many of the emerging applications also come with some drawbacks. Given the transnational nature of blockchain technologies, malicious individuals can exploit them for illicit transactions. This factor, along with the pseudonymity provided by blockchain, can make complicated for law enforcement agencies to identify and prosecute these kinds of users. As more and more communities form their own values, individuals' behavior will become harder to regulate through external forces imposed by third parties (such as national laws). And if the law becomes less efficient in its capacity to administer, governments will be forced to regulate by intervening into markets or by revising the code design.

Within a decentralized context, states and governments would need to adopt a different approach to shape markets. As of today, marketplaces backed by DAOs will not allow government intervention. Laws which try to prevent anticompetitive practices, become more difficult to enforce. Besides, the open nature of blockchain-based applications lets anyone to reproduce or adjust most of them, for satisfying the interests of the different communities. In this regard, states can always adopt coercive measures in order to force users to update their clients. Yet, regulating a blockchain-based architecture can be a tricky task, since there is the concrete risk of undercutting the powerful interconnectivity of the Internet and the typical notions of free expression. For this reason, if we want to preserve the upsides provided by the blockchain technology while reducing to the minimum their possible drawbacks, we have to start thinking about a new law archetype. This new legal model should be able to balance the power of the Blockchain in such manners to promote economic growth, free speech, and the protection of individual rights and liberties.

2.4. GDPR: can DLTs be squared with the European Data Protection Law?

Over the past few years, blockchain's potential for the EU's Digital Single Market[15] has been at the center of many debates. By its nature, indeed, this technology seems to be unable to comply with the European data protection law. This paragraph aims to analyze the relationship between the blockchain technology and the GDPR (General Data Protection Regulation)[16], pointing out the present tensions and the possible future solutions.

[15] The European Union's "Digital Single Market" designates the 2014-2019 strategy of the European Commission for the best possible access to the online world for individuals and businesses.

[16] The "General Data Protection Regulation" (GDPR) is a regulation on data protection and privacy in the European Union (EU) and the European Economic Area (EEA), which also addresses the transfer of personal data outside the EU and EEA areas.

The GDPR is based on the 1995 Data Protection Directive[17] and became binding in the year 2018. On the one hand, it facilitates the free movement of personal data within the area of the European Union. On the other side, it institutes a legal framework for the protection of certain fundamental rights, which builds a set of obligations for data controllers (the bodies that determine the means of data processing).

The aforementioned clashes between blockchain and GDPR depend on two preeminent elements. Firstly, the GPDR is based upon the principle for which, with respect to any personal data, there is (at least) one person (either natural or legal) whose data subjects can address to accomplish their rights. However, blockchains are designed to reach decentralization for replacing a single player with more actors. And this renders burdensome the allocation of accountability and responsibility in relation to the not-so-clear concept of "joint controllership" under the current regulation. For this reason, a further complication arises due to the loss of legal certainty concerning the definition of entities qualify as "joint controllers". Secondly, the GDPR is based upon the presumption that data can be modified or deleted whether necessary in order to comply with the legal requirements provided, for instance, by articles 16 (for which data must be amended) and 17 (for which data, in some cases, must be cancelled) of the regulation.

Such data modifications are made onerous by the blockchain not only in order to achieve trust in their network, but also for assuring data integrity. Nevertheless, the general uncertainty regarding blockchain technologies is boosted by the already existing uncertainties related to the current European data protection law. There is an ongoing debate with respect to when (hashed or encrypted) data stored on a distributed ledger can be qualified as personal data for the purpose of GDPR. Another example is referred to data minimization and purpose limitation. While GDPR requires that personal data must be processed just for means and purposes specified in advance, these two principles are arduous to apply to a blockchain technology, since DLTs are append-only databases which continuously grow as new data are added.

Additionally, such data are replicated on several computers. Therefore, it is problematic from the data minimization's viewpoint, and it is unclear how the personal data processing's mean should be applied to the blockchain as well. The most debated aspect in relation to blockchain technologies is perhaps the "right to erasure" (also known as the "right to be forgotten"), since they often make the

[17] The "Data Protection Directive" (Directive 95/46/EC) was an EU directive which aimed at regulating the processing of personal data within the European Union and their free movement.

data modification complicated if not even impossible. Again, this is hard to conform with the requirements provide for by articles 16 and 17 of the GDPR.

This analysis drives us to draw two major conclusions. In the first place, that the governance and the technical features of the blockchain's use cases can be difficult to fulfill the GDPR's requirements. In the second place, this lack of legal certainty could lead to other issues related to technology in general, and not only in relation to the specific characteristics of the blockchain technology. As of now, the current EU's data protection regulation seems to be not able to determine how it should be applied to these techs.

Let us evaluate the European data protection law's factors relevant for the blockchain. In order for us to do so, we have to include: the definition of responsibility of the actors who may be qualified as data controllers, the core principles of personal data processing to blockchains, the implementation of data subject rights across such networks, the material and the territorial scope of the regulation, and the international data transfers with the data protection impact assessment. It is still disputing whether blockchain might be a suitable instrument for realizing some of the GDPR's goals, since blockchain technologies are tools which support alternative forms of data-sharing management and distribution with respect to other already existing techs.

Moreover, beyond data-sharing, blockchain have the potential to influence the contemporary data economies. Through the support of the development of the artificial intelligence within the European Union, for instance. Specifically, DLTs could be useful for supporting the GDPR in the achievement of their objectives, such as the right of access (Art. 15) or the right to data portability (Art. 20). Furthermore, they could be used to give more control on personal data and help with the detection of data breaches or frauds. To this end, there could be applied some policy options:

a. Regulatory Guidance

First of all, the key point is tied up to the legal uncertainty surrounding the current European data protection law and how it should be applied to the blockchain technology. We saw that blockchain's technical structure and DLTs' data governance are, usually, in contrast with the GDPR's requirements. Even attempting to regulate blockchains show a greater uncertainty concerning both application and interpretation of the legal framework. Nevertheless, the GDPR has not to be necessarily revised. The regulation is an expression of principles-based law, designed to be neutral. But, with the occurrence of new technologies, it needs to increase legal certainty by means of a new (and clear) regulatory guidance. Supervisory authorities could coordinate action with the European

Data Protection Board[18] in order to outline a specific guidance on the application of the GDPR to the blockchain. Yet, some of the Article 29 Working Party (Art. 29 WP)[19] options, not endorsed in the past, could be even advantageous for the blockchain industry. Therefore, on one hand, a regulatory guidance could offer further certainty to the ones who desire to operate in the blockchain space. On the other one, it could bring more transparency to the broader data economy marketplace.

b. Support Codes of Conduct & Certification Mechanisms

The GDPR was thought to enable its application to any tech, regardless of the specific use cases. The GDPR's technology-neutrality, however, means that (sometimes) can be challenging to apply it to certain cases of personal data processing. Anyway, the GDPR's codes of conduct and certification mechanisms are aimed at helping to apply their principles to those backgrounds where personal data are processed. Besides, they also support European data protection law to guarantee t its personal data processing's assumptions, improving, for example, cloud computing systems.

c. Research Funding

Even if certification mechanisms and codes of conduct (along with a new regulatory guidance) would surely help to attain much legal certainty, this will not always be enough to enable compliance of a determinate distributed ledger use case with the GPDR. In some cases, indeed, there could be technical limitations which obstruct that compliance. In other situations, instead, the designed blockchain's governance is unable to compliance with the legal requirement provided for by the GDPR. At this point, solutions could be encountered through a deep interdisciplinary research funding, trying to find governance and technical remedies to the current blockchains' protocols.

[18] The "European Data Protection Board" (EDPB) is an independent European body whose purpose is to ensure consistent application of the GDPR and to promote cooperation among the EU's data protection authorities.

[19] "The Working Party on the Protection of Individuals with regard to the Processing of Personal Data" or (more simply) the "Article 29 Working Party", was an advisory body composed of a representative from the data protection authority of the EU Member States, the European Data Protection Supervisor and the European Commission.

2.5. The "Blockchain Antitrust Paradox": does Blockchain represent the Death of Antitrust Law?

Numerous institutions, including the Organization for Economic Cooperation and Development (OECD)[20], have identified the need to address the antitrust challenges generated by the blockchain technology. Above all, one is suggested by the word "antitrust" itself. On one side, much of competition law is articulated as anti-trust. On the other hand, as we know, blockchains eliminate the need for a fiduciary (a person who creates trust). So, what happens when antitrust law contemplates a technology that works without a trusted counterparty? And, from a legal perspective, are the current rules suitable for the blockchain?

Answering these questions could present a significant risk of inaccuracy, but it is essential to do so before existing models of antitrust enforcement become obsolete. The Internet world has stressed the legal system by substantially increasing the velocity at which law must be applied. Anyway, with the blockchain, it is not just about speed. The very nature of this technology, indeed, raises other crucial questions about antitrust law and how individuals conduct transactions. Here, in particular, our intention is to assess the challenges that blockchains can produce by analyzing unilateral anticompetitive practices and proposing some changes to the current antitrust law. In this regard, let us divide the discussion into three main parts.

Firstly, let us debate that several challenges arise with respect to the ability to detect anticompetitive practices and in relation to their perpetrators. Secondly, let us argue antitrust laws and how they could (properly) regulate the blockchain. Some legal remedies, for instance, cannot be used to prevent the development of anticompetitive practices implemented through it, due to the very essence of the technology. It addresses how antitrust authorities should cope with these issues. Lastly, our dilemma is: does blockchain represent the death of antitrust law? Since blockchains are continuously evolving technologies, answering this is not an easy task. The decentralized nature of this tech forces us to consider the legitimacy of antitrust law, which is still based upon centralized legal structures, but at the same time it is still needed. That is what, in this paragraph, we name the "blockchain antitrust paradox".

One of the key antitrust law problems related to the blockchain is the detection of anticompetitive practices, as well as the identification of those who engage in them. Algorithms drastically accelerate a company's ability to engage in anticompetitive practices, while limiting the antitrust authorities'

[20] The "Organization for Economic Cooperation and Development" (OECD) is an international organization whose main purpose is to improve the global economy and to promote the world trade.

ability to detect and gather evidence of them. Outside the blockchain environment, when algorithmic anticompetitive practices are recognized, the perpetrator is generally known as soon as the practice is identified since her/his identity is not protected. Within the blockchain ecosystem, instead, things are different. As previously explained, through pseudonymity, this technology ensures the privacy of its users. These nodes produce obstacles to the law enforcement.

For this reason, tracking services are being developed (even though they only work on some blockchains). Tracking services are likely to improve, but at the same time, new technologies are being developed to protect users' real identity. Concerns which predict the end of pseudonymity should, therefore, be kept in mind. There are two different paths in the blockchain sphere currently. One involves working with governments in order to develop legally compliant blockchains, in which pseudonymity may disappear. The other one involves developing a system where everything in blockchains is encrypted, even the number of transactions. The point is that, on this subject, these scenarios lead us to believe that technology will move faster than policymakers. Besides, the blockchain constitutes a mere barrier to antitrust enforcement because of the distributed system of its network architecture. Nobody is in control of public (permissionless) blockchains, but at the same time everyone is. Accordingly, even if a practice is identified as an anticompetitive one, it actually cannot be stopped.

Again, blockchain is immutable. Meaning that once information is stored on it, it is not possible to erase it. Since this tech is governed under the lex cryptographia, it will continue to function as long as its participants pay the transaction fees charged by miners. Dapps (Decentralized Applications)[21] cannot be shut down because there is no server to close. In other words, if an anticompetitive smart contract is implemented, the blockchain will continue to perform the transactions anyway. As a consequence, even if antitrust agencies will find a way to identify an anticompetitive practice, there is no directly enforceable solution. This possibility has led some people to ask for regulatory instruments which could be used to prevent abuse of dominance. Nonetheless, these proposals would require outlawing dominant positions, something inconsistent with the principles of antitrust laws that just sanction abuse of dominance. Therefore, such a proposal should not be adopted. However, since antitrust law contribute to consumer welfare, there must be a way to prohibit anticompetitive practices occurred on a blockchain.

[21] A "Decentralized Application" (Dapp) is a computer application which runs on a distributed computing system.

As of today, effective ways to apply antitrust law to blockchain are yet to be found. In order to avoid drastic measures which could jeopardize individual freedoms, regulators should foster blockchains to be designed in compliance with the "law is code" approach. The idea that "code is law" remains useful in understanding the blockchain technology and what regulators should seek: influencing the design of this technology. Nevertheless, blockchain characteristics allow the spread of illegal activities and so the "code is law" approach must be supplemented with thr "law is code" one, which explains how the regulator should act. For the first time in history, it appears necessary to integrate legal requirements into the technology itself. Without implementing such an approach, technological barriers will deprive the law of any effect. Blockchain creates a technical fortress, and the practices that are carried out inside (or via) blockchains are well-protected. Fortunately, there is a way for antitrust law to tackle this issue, thereby providing a role for legislators to supplement antitrust laws. With no regulation, it will be impossible for the law to catch up with the technology. An effective regulation is essential in this space, although lawmakers must proceed with extreme attention. They should respect five founding principles that shape the blockchain technology:

I. Pseudonymity

Since imposing regulations that mandate disclosure of users' identities would be contrary to the blockchain's very nature, it will actually eliminate an alternative model to most of the modern technologies where real identify of users is known and monetized.

II. Distributed Architecture

This blockchain core element generates distributed power, meaning that no central point of failure exists and the harm from one user's irresponsible behavior is contained solely to that person.

III. P2P transmission

The existence of a Peer-to-Peer transmission system among users must not be challenged by regulations. Doing so, would be equal to reintroducing middle-market firms into the blockchain world, unnecessarily making blockchains less attractive.

IV. Consensus

Creators must remain free to choose the consensus mechanism they wish to utilize. Therefore, blockchain users should be free to participate in the block validation process they prefer, without becoming liable for assenting to an anticompetitive practice the blockchain could be involved.

V. Immutability

Enabling an entity to delete data or stop transactions on a blockchain would undermine trust, that is a vital aspect on which the blockchain is based.

Regulations which challenge one of these five principles could cause blockchain to lose its utility. The way this tech will evolve is uncertain, and choices made by their communities will fundamentally affect which values are built into it. For this reason, it is intriguing for regulators to get involved in how this technology will turn out. These issues are too important not to let blockchain technologies' transformations emerge on their own. In light of such landmark principles, regulatory humbleness will have to ensure that blockchain continues to develop to its full potential.

Anyway, it is clear that allowing blockchain technology to emerge does not mean that nothing should be done about the potential illegal practices implemented on it. Despite the central blockchain's pseudonymity principle, the identities of users engaged in anticompetitive practices will be reported to antitrust authorities. This situation occurs when the real identity of a user is known to other ones. Thus, pseudonymity does not protect blockchain's users against all types of detection and identification. The anticompetitive effects caused by one practice on the market may also lead an antitrust authority to launch an investigation. Since real identity of users or blockchain creators is not always known, only a "law is code" approach here will enable courts to enter the blockchain technology.

Two challenges then come up: one regarding the applicability of legal requirements, one concerning the necessity not to hinder blockchain technology's key features while making the law effective. Imposing fair regulatory mechanisms to blockchain communities, thanks to the implementation of code, will only be successful if developers and users are incentivized to comply with the law. The policymakers' ability to impose legal requirements, indeed, is not effective on the blockchain because its creators are covered by their pseudonymity. In other words, law must not be conceived as a threat, but rather as an ally of the blockchain. Both developers and users must agree to facilitate legal enforcement by integrating the code proposed by the regulator.

New mechanisms must be developed in order to identify malicious behaviors and to make sanctions effective. To this respect, legislators may incentivize the implementation of apparatus allowing a qualified majority of nodes to vote for revealing the identity of another node (within private and permissioned blockchains). This would be consistent with the concept of decentralization behind the

blockchain by preserving the will of the majority. As far as also public blockchains are concerned, different types of governance might be promoted by establishing certain "safe harbors" for specific configurations in the blockchain code in order to make it harder to use it for illegal purposes.

Alternatively, self-regulation and co-regulation should be considered as well. With respect to the remedies, a real challenge is generated by the absence of "choke points" on the blockchain. Its structure makes difficult to apply injunctive relief, since it is nearly impossible to enjoin a decentralized and autonomous organization. The only viable option seems to embed regulatory measures into the blockchain's governance. Another voting tool here could be developed in relation to the creation of forks, determined by courts or antitrust agencies. Hence, a delicate balance between the "law is code" approach and the need to protect the most important principles of blockchain must be found. Time will show which tool will be appropriate in specific situations. In any case, a "law is code" approach seems inevitable given the fact that antitrust law (if maintained like this) will quickly become ineffective for technical reasons.

The necessity to control anticompetitive practices will lead to many policy discussions. If a government decides to regulate blockchain too strictly, innovation will be harmed as developers could move away to other less regulated technologies. Since the future evolution of the blockchain technology is still unknown, it is not simple to evaluate the scope of such practices. However, most of the usual tools of antitrust law will be ineffective in the face of blockchain. Current antitrust law, indeed, may soon be ignored. Three main factors validate this hypothesis:

First, without regulatory infiltration, antitrust law will probably become ineffective. For the first time in its history, it will have to be supplemented by regulations based upon a "law is code" approach. Antitrust laws must tackle issues concerning how to detect the anticompetitive practices committed on the blockchain, how to identify responsible actors, and finally how to remedy them for the future. While the author of an anticompetitive blockchain can sometimes be identified, the effectiveness of sanctions may be stop by immutability. Hence, even where antitrust law will find a correct way to regulate blockchains, it might expire since it is no longer a creator of welfare by itself.

Second, public (with no permission) blockchains will limit monopolization even if new governance tools will be adopted. Moreover, since the transactions implemented on public blockchains are visible to all, the incentive to engage in anticompetitive practices is reduced since market surveillance and industry monitoring can incur illegal activities. However, some perpetrators will be protected by the

“opacity effect” created by the blockchain’s characteristics. This is particularly true for private blockchains, where absent regulation infiltration is technically impossible.

Third, to expect the death of antitrust law seems to be bound to its foundations. There is no doubt lawmakers will find new manners to submit blockchains to the law. However, the regulator could end up protecting the existence of antitrust law, even though its initial goals are no longer the same.

Besides, the death of antitrust law might not be only linked to blockchain’s technicalities. Its destiny may also depend on the conflict between the logic of blockchain technology and the logic of antitrust law. As a matter of fact, the blockchain technology challenges the reason for being of the antitrust law. Conversely, antitrust law was born for (and applied by) centralized regulatory agencies and the European Commission. Enforcing antitrust law amounts to imposing vertically designed rules on a technology built around the desire for decentralization. This opposition between the vertical mean of antitrust law and the horizontal one of blockchain raises also a legitimacy concern.

The cultural and sociological factors which have brought to the development of blockchain technology cannot be ignored by the law. In order to address this, a solution for decentralizing antitrust law and authorities should be found. Therefore, they can no more neither rely on pyramidal structures nor continue to operate in a closed circle on the model of nation-state-led government.

CHAPTER 3 – Shaping the European Digital Future: a New Governance for EU

3.1. A Short Premise

Once described in detail the main features and the most relevant legal facets related to blockchain and smart contracts, it is time to try to figure out their future within the European Union's landscape. To do so, we first explore the case of Malta (one of the most developed and advanced European countries on the blockchain level); we then make an intercontinental comparison (in the second-last paragraph of this chapter), illustrating the remarkable 13 blockchain-enabled laws enacted in the American state of Wyoming; and, conclusively, we broadly outline the regulatory approach adopted by the EU for facing the new digital challenges. Respectively, while Wyoming is the classical example of "blockchain-friendly" state from which other federal states could learn, Malta exactly represents the European paradigm which the Member States should follow. However, despite the latest legislative proposals, Europe is still far behind USA in this respect.

3.2. Blockchain & DLTs for a Digital Government: The Maltese Case

"To ensure fast access to regulated information on a non-discriminatory basis and make that information available to end users, the European Securities and Markets Authority (ESMA) has an obligation to develop and operate a European Electronic Access Point (EEAP)". [22]

Let us start with this statement, a requirement of the Commission Delegated Regulation (EU) 2016/1437, which aims at enabling better accessibility and transparency to a comprehensive set of information about European listed companies for potential investors. The European Financial Transparency Gateway (EFTG) pilot, undertaken by the "Directorate-General for Financial Stability, Financial Services and Capital Markets Union" (DG FISMA), has demonstrated the capacity for a blockchain or a Distributed Ledger Technology to ease the EEAP requirements and furnish concrete benefits for those stakeholders impacted by the Transparency Directive (also called "Transparency Obligations Directive" or "Directive 2004/109/EC"). Nevertheless, establishing governance for a DLT or a blockchain enabled EEAP solution seems to be still a difficult challenge for the European Union.

[22] "Governance for a DLT / Blockchain enabled European Electronic Access Point (EEAP)" – European Commission (Final Report, October 2019)

Building a powerful governance organization is crucial for the success of that solution, even though achieving the level of collaboration required from the participants is challenging. An effective governance in a DLT network relies more on people than the technology itself. Figuring out Officially Appointed Mechanisms' (OAMs)[23] interest for participation is essential, as they must be willing to put effort and resources for supporting the initiative. Indeed, the road that leads to the implementation of a DLT/Blockchain enabled EEAP will mainly depend on ensuring an early commitment from the OAMs, and reaching an agreement concerning the core technology decisions. The establishment of an OAM ecosystem would require lots of time and fatigue, and the success of these activities would bank on the elements of governance and decision-making.

Additionally, we can say that digital governments represent the modern paradigm of the public administration sector. They mainly focus on a user-centric provision, along with rapid and innovative public services. Such services should leverage digital technologies, as well as governmental and citizen information assets. Blockchain is definitely one of the most cutting-edge techs which have to be considered under the new governmental policy making and service delivery models.

Within this context, such a technology has the power of facilitating direct interactions among public institutions and citizens. In particular, the blockchain is a combination of disparate already existing techs which design a new distributed information infrastructure. Decentralization is the central characteristic that can reshape the way governments interact with the citizens. Blockchains could cover a consistent part of the administrative tasks currently fulfilled by a government. The latter should not provide information storage and information exchange processes on its own. Instead, it should maintain a kind of supervisory role on the transactions taking place on a blockchain network. Moreover, blockchain technologies can potentially be used as an infrastructure for exchanging information between public administrations. Greater reliability and improved performance are particularly important when applications require data from multiple sites, organizations or states.

Blockchain is also promising from a citizen-centric perspective. Services drawing on decentralized nature of blockchain (such as identity or voting) change a balance of power, increasing the citizens' ownership and control. The architectural structure of the blockchain can reduce operational risk and transactional costs, increase trust, and compliance in government institutions as well. However, the lack of stable commercial platforms and the loss of actual implementations within the current

[23] The term "Officially Appointed Mechanism" (OAM), used throughout Europe, refers to national databases for regulated financial information.

governments indicate that this tech has yet to mature. Concerns often highlighted are not only related to governance, but also to scalability and flexibility.

The EU's strategy is designed to fill these gaps. Specifically, Europe provides a "gold standard" for blockchain technology, embracing the European principles with its legal and regulatory framework. The gold standard includes goals like interoperability, environmental sustainability, data protection, cyber security and electronic identification. The European Union is trying to support blockchains on policy, legal and regulatory levels. The most significant parts of the strategy are:

- Building a Pan-European public services blockchain
- Promoting legal certainty
- Increasing funding for research and innovation
- Promoting blockchain for sustainability
- Supporting interoperability and standards
- Supporting blockchain skills development
- Interacting with the community

Coming to our case, in October 2017, the Maltese government launched a project for developing academic credentials verification using the blockchain technology. The Ministry for Education and Employment (MEDE) of Malta decided to adopt the so-called "Blockcerts", an open standard for building applications that issue and verify blockchain-based official records, designed in 2015 by the Massachusetts Institute of Technology (MIT) and a startup called Learning Machine. Let us explain how this open standard works hereunder:

a. Functionalities

Among the most important functionalities there is the issuance of academic credentials, the verification of certificates, and the storage of personal credentials in the user app. The Blockcerts application provides a wallet where a citizen has the full ownership of her/his records. This system allows the citizen to control which third parties can see the academic records and verify originality. Verification can be carried out via the Blockcerts universal verifier, a webpage accessible for all. Through the URL of the certificate, one can verify the validity of the certificate and other relevant information.

b. Governance

It is a hybrid consortium. The abovementioned MEDE is the main sponsor of the pilot and Learning Machine is just one of the technological partners which implement the Blockcerts code, since there are many other parties involved. Anyone who has credentials of one of the consortia partners can utilize the service.

c. Usage

Since the Blockcerts open standard is still being developed, the Maltese pilot project has still a small scale. It only includes two educational institutes with their students. Over a hundred credentials have been issued at the moment, while the number of verifications performed by third parties is unknown. Besides, the Blockcerts standard issues hashes on the blockchain in batches, allowing for scalability on the Bitcoin platform as well.

d. Technical Architecture

The private blockchain network is made up of the certified institutions that participate in registering the academic certificates. At the same time, the open standard leverages public blockchain networks, as it anchors hashes of the certificates on the Bitcoin platform. The DLT layer of the solution uses the classical Proof of Work consensus mechanism. Apart from Bitcoin blockchain, much of the community effort is currently going into creating Ethereum interoperability.

e. Costs & Benefits

Regarding the benefits for the end users, we can find:

- Credentials' ownership for the citizens
- Self-sovereignty: the permission to share is placed at the citizen instead of the institution.
- Identity and privacy protection: citizens can choose to share certain certificates with specific institutions.
- Convenient storage and sharing, quick verification of certificates: no need for hard copies anymore, and no more risk of using a fake certificate.

Concerning the costs, we have:

- Standard development cost: the Maltese government is willing to finance the development of the Blockcerts open standard and intends to extend this pilot for all academic issuing institutions.
- The cost-of-service implementation and integration: technology developers take charge of huge building costs of an automated credential process for several consortium partners.

Furthermore, the year after the adoption and the implementation of the Blockcerts open standard, the Malta Digital Innovation Authority (MDIA) was introduced with the explicit purpose "*to promote consistent principles for the development of visions, skills, and other qualities relating to technology innovation, including distributed or decentralized technology, and to exercise regulatory functions regarding innovative technology, arrangements and related services and to make provision with respect to matters ancillary thereto or connected therewith"*[24].

Its first policy action was to create a new regulator for the Innovative Technology Arrangements (ITAs), and it was not set up for regulating cryptocurrencies, but rather for addressing technology agreements that constitute blockchains, smart contracts and other DLTs. Generally speaking, many people disagree that technology should be regulated at all, let alone have a self-standing regulator for such a new sector. Nonetheless, the reason why the decision to take this step was taken relates to the fact that this technology has decentralized governance's features which make it different from every other tech. Most importantly, the Government of Malta recognized that once deployed, this technology could be in breach of the law. Therefore, a call for redress was needed. The result of this law was to ensure that the technology passed some quality tests on some important aspects covering vulnerabilities. The creation of the Malta Digital Innovation Authority is also important to grant that limited resources in this field are concentrated with a clear agenda. That would avoid overlaps with other existing regulatory authorities. It also seeks to prevent duplication and contradictory strategies, while maintaining expertise on a subject matter combined with knowledge and awareness of the strengths and weaknesses of Distributed Ledger Technologies (DLTs)

The Innovative Technology Arrangements and Services Act (ITASA), instead, is the law that introduced the initial licenses for which one could apply. It does not decide that one needs a license to deploy blockchains, DLTs or smart contracts. What the Act seeks to do is to offer certification to a developer of an innovative technology arrangement which can provide trust in the market, and it is

[24] Malta Digital Innovation Authority Act (MDIAA), Chap. 591, Laws of Malta.

voluntary. This voluntary nature of certification tries to address two main issues. The first one is that this is a newly charted territory. Anyone offering software facilities, in the private sphere, will warrant their qualities as part of the offering for sale or lease. That produces a buyer of the software and liability for deficiencies, otherwise a lessee will be able to rely on the warranty and sue for damages in case of software failure. Systems auditors are registered with the MDIA, following an application process that involve a sort of due diligence exercise, including the scrutiny of their subject matter experts. Once registered, they can be engaged by a developer or (indirectly) via the technology arrangement in order to review the software. It will then lead to certification by the authority, whenever the requirements standards are met. As of today, certification of an innovative technology agreement can take forms for DLT (both alone and with smart contracts), or just smart contracts by themselves.

Another essential service provider is the technical administrator, conceived for playing a potential role in the post-deployment and certification processes. The technical administrator, indeed, must be the last recourse point. If no one acts to fix a problem (like infringement), then the technical administrator must intervene. In order to effectively do so, the software must give her/him some powers. Such interventions will vary depending on the type of arrangement. However, this could range from the ability to update smart contract logic (which could be based upon a governance structure) to the issuing of software updates, for example.

Systems auditors are required to assure that all the information is recorded in real-time through a technology blueprint, without the risk of omission or corruption. The legislation, then, aims to address the problem of the identification of owners and controllers of the arrangement. Anti-money laundering laws, privacy laws and consumer protection laws assume traditional corporate operators where the process of identification is quite simple. Tokens have challenged all that. Some of these solutions have been integrated in the law for supporting anti-money laundering, along with the simultaneous introduction of tax guidelines.

3.3. The Status of Initial Coin Offerings (ICOs) within the EU

The issuance of digital tokens, based on the blockchain technology, is an innovative method in order for firms to raise their capital. Since today almost everyone can participate as an investor via the Internet, the so-called Initial Coin Offering (ICO) simplifies this process. An Initial Coin Offering (ICO) is a relatively young but already very famous blockchain-based financing option, in which new coins are issued on a blockchain and transferred to investors in return for capital transmitted as

cryptocurrency. In particular, it represents a digital way of public capital funding for entrepreneurial use, through the issue of own virtual tokens.

ICOs have become a growing and convenient way for startups for funding capital. This is an enormous opportunity for small private investors, who have hardly access to traditional financing forms. Cost optimization, of course, is another great advantage. In fact, it is possible to carry out an ICO without any intermediaries, and therefore to run an ICO at much lower costs. While a complex IPO (Initial Public Offering)[25] often takes a long process, an ICO can be concluded in a shorter time. Typically, the key ICOs elements are fully automated on smart contracts, containing features of the abovementioned IPOs crowdfunding and venture capital (VC) at the same time. The strong movement towards disintermediation of traditional funding agents and financial services in general, has led ICOs to the disruption of the established funding system.

Nevertheless, ICOs have been neglected by research so far, and they are not as well-understood as related established investment models. Many countries have begun to try to issue initial regulations, with consequent either clarification of already existing laws in some places or complete banning in other parts. While uncertainty and (as of now) inexistent regulations are responsible for this boom, a precise regulatory treatment of tokens will be pivotal for the success of the legitimate token-issuing in the near future. The comparison of several regulatory frameworks identifies different approaches concerning the ICO phenomenon on a state-by-state basis. The potential international cooperation could promote appropriate regulations, fostering a worldwide spread. Clarity with respect to the way tokens are dealt with and the opportunity to receive feedback from the regulator provide a high level of legal certainty. Nonetheless, a proper regulation is not the only missing element which is determinant for the attractiveness of certain locations.

With the deployment of own tokens, startups can provide rights and obligations for their token owners. Due to the development of the Ethereum platform, it is possible to create a token carrying out an ICO with (approximately) 100 lines of programming code. The procedure is usually as follow. The token designer normally publishes a white paper with the fundamental terms. This paper is commonly disclosed on online channels, such as crypto forums and websites. After that, the token is sold to anybody who is willing to invest in the project. To this end, the investor needs to transfer cryptocurrencies to the issuer's wallet in order to receive the new token. The purchase price of the

[25] An Initial Public Offering (IPO) or "stock market launch" is a public offering in which the shares of a firm are sold to institutional investors.

token is not part of the equity of the company, but it represents capital that this firm collects without diluting its own equity structure.

However, ICOs are not always a suitable way of raising capital for every kind of business. Large enterprises still require more sophisticated contracts, for instance. Although blockchains are fundamentally unsuitable for laundering funds and financing illegal business actions because of its nature, they are frequently associated with such activities due to the anonymity of the transactions executed across their networks. Then, there are also risks concerning cyber security. While the blockchain itself is extremely forgery-proof, the most vulnerable points for criminal operations lie in the input and output interfaces. The issued token can be listed on the so-called digital currency exchanges (DCEs), that are organizations which enable their consumers to exchange virtual currencies or tokens for other assets (like legal tender or for other digital currencies).

Yet, the need for stronger and clearer regulations is perceived negatively by a significant number of blockchain's members. This can be explained by the fact that the original concept of a decentralized network was intended to oppose centralized authorities. However, unregulated market environments will no longer be preferred. Transparent policies legitimize crypto operations and reduce the problem of scams in the crypto ecosystem. Such a legitimacy could lead to new funds from institutional investors in this sector. As a result, innovation can speed up even more. At a national level, there are more efforts concerning ICO regulation. Many countries handle the issuance of tokens differently. While some jurisdictions try to regulate ICOs with already existing laws, other countries issue new ICO specific guidelines and actively support the blockchain. Depending on the country, there are discussions and warnings to take an active position or no acting at all. Not only nations and authorities are keen to provide regulation on ICOs, the ICO industry and their issuing firms are interested in precise regulations as well. All the members commit themselves to a code of conduct, which obliges corporations to comply with ethical principles and a greater due diligence in order to prevent illegal acts in a more effective manner. The process of ICOs consists of three main stages: the planning phase (pre-ICO), the token sale (the ICO itself) and the post-ICO.

- The Planning Phase (Pre-ICO)

The first passage can decide whether an ICO succeeds or fails. In order for an ICO to be successful, it requires clear objectives and a careful preparation. The starting point for launching an ICO is the idea of the firm. This idea should be technologically feasible and able to become a marketable

product. In addition, companies have to take into account if an ICO is suitable for their business. As tokens can be under pressure after their emission, the business model should be sustainable. Therefore, it is advantageous when tokens are an integral part of the product, and the business model is blockchain-based.

- Token Sale (ICO)

Some corporations decide to start a pre-sale, before beginning the public sale. A pre-sale usually has a lower total funding amount than a public sale and gives an incentive to early adopters by offering tokens for a lower price. One of the leading objectives of a pre-sale is selling a package of tokens to venture capitalists (or other institutional investors) in order to stabilize the tokens value and for increasing the credibility of the ICO. Through a pre-sale, businesses can cover some of the costs for the actual public sale. Furthermore, they have the opportunity to determine the demand and the appropriate price. Once the tokens are sold, investors generally send funds in form of cryptocurrencies to a determined wallet address. Cryptocurrencies are transferred from the wallet of the investor to the wallet of the firm, usually by means of a smart contract. In case of the pre-specified funding volume is accomplished within time, the ICO is successfully completed. A very common approach related to the tokens' distribution is to create pre-functional tokens only for the issue and trade on secondary market exchanges. Another approach, instead, is to record sales and deliver tokens once the network is functional. Specifically, the distribution of the token works as follows. The deterministic algorithm of a smart contract first automatically and directly pays the acquired tokens to the investor's wallet. Depending on the token type the investor can use the tokens differently. Typically, some of the tokens are reserved by the firm for founders and employees. Just a few companies allocate the reserve to non-profit foundations.

- Post-ICO

Even in the post-ICO, the trade of tokens on cryptocurrency exchanges is still possible. Businesses invest the acquired funds into product development. It is important to constantly inform investors about the course of the project, maintaining continuous communication on each channel. Before and after the launch of the product, performance monitoring is also important to ensure the corporation's sustainability.

In 2018, the Securities and Markets Stakeholder Group (SMSG) published a very important report about ICOs named "Own Initiative Report on Initial Coin Offerings and Crypto-Assets", set under the European Securities and Markets Authority (ESMA)[26] regulation. SMSG, in particular, helps to ease consultation between its own board of supervisors and shareholders on ESMA's areas of responsibility. Specifically, within the statement, SMSG gives aid to ESMA on those crypto-assets which could bring risks to investors or financial stability.

Furthermore, SMSG divides the different ICOs legislations of the European countries into three main categories with three different approaches: proactive approach, careful consideration and undefined approach (or non-active approach). Among the European states which share between themselves legislations with an evident proactive approach, we can find, for instance, Malta (whose example has been explained in the first paragraph of this chapter) and Switzerland. The countries associated with the second group (such as Austria, Belgium, Germany, Portugal and Spain), instead, have chosen to follow a measured approach in order to assess ICOs on a case-by-case basis, without restricting or prohibiting them. While, as to the last third and last class (like Croatia, Greece, Italy and Sweden), they have not yet determined clear information on how to regulate ICOs. However, this does not mean that Initial Coin Offerings are either utterly allowed or wholly banned.

Therefore, the SMSG's country overview focuses on the presence of many different approaches with respect to ICOs' and crypto-assets' legislations within the European Union. According to SMSG, the missing regulations impede the formation of an internal ICO market. SMSG is also recommending ESMA to clarify the application of existing financial regulations to virtual assets. Moreover, the adoption of distinct national approaches in the EU, instead of regulations homogeneously implemented on a European level, will result in the emersion of certain European countries as much more innovative than others. That would generate a heterogeneous business environment for companies operating on several diverse European jurisdictions, leading also to different investor protection standards. It may even happen that firms planning to issue ICOs could avoid distributing their tokens throughout Europe.

[26] The "European Securities and Markets Authority" (ESMA) is an EU financial regulatory agency and European Supervisory Authority, which replaced the Committee of European Securities Regulators (CESR) on 1 January 2011.

Besides, in the so-called "2019 annual working program", ESMA states its aim to reach a coordinated approach for harmonizing the governance of new financial activities. Some ICOs, indeed, resemble financial instruments. Nevertheless, due to the flexible nature of token design, there is the problem that some ICOs would not fit into the classification and so would not be affected by the legal framework. This is because there is no encompassing EU legal framework including all ICOs. Some regulators are hence in favor of general guidelines, while considering the tokens' classification in security and utility ones. In case of ICOs security tokens, consistent laws can be applied. Regulations for utility tokens, which are currently the most popular form of tokens, remains rather still unclear.

As to the secondary markets for the trading of tokens, there are some already set (and regulated) cryptocurrency exchanges which comply with applicable laws. Nonetheless, most tokens issued through ICOs are not tradeable on established exchanges. These exchanges are often affected by further risks, like trade-based manipulation. As a result, the internet community often perceived ICOs as non-regulated. Thus, the applicability of EU and legal law is obviously contradicting with the general idea of issuing ICOs via the Internet. For this reason, ICOs need to be reviewed in detail and checked whether they fall under the definition of specific regulations. This procedure could be unclear and complicated for issuing enterprises, as well as for investors. This makes issuing tokens in several European states difficult for corporations, because many different legal frameworks have to be still considered and understood.

3.4. Legal Regulation of Cryptocurrencies in Europe

As blockchain technology is continuously evolving, the European cryptocurrency market is constantly increasing as well. So that several regulations (and concerns) are advancing on a daily basis. As of today, the European regulatory framework for digital assets has been driven by individual countries, which have made their own rules and have taken decisions by themselves. However, Europe has (slowly) started to show a certain interest in harmonizing the legal regulation of digital assets within the EU.

For instance, in January 2020, the "5th Anti-Money Laundering and Counter Terrorist Financing Directive" (5AMLD) has been adopted by the European Union in order to contribute to global security and to integrity of the financial system, grasping crypto with the new definitions of "virtual currency" and "virtual asset service providers" (VASPs). Under the legislation, cryptocurrency businesses are now considered to be obliged entities, just like typical financial institutions. Some months later, the European Commission proposed the "Markets in Crypto-assets" (MiCA) with the

goal of coordinating a comprehensive regulatory framework for digital assets and their service providers across the EU. MiCA will introduce standardized definitions for some specific digital assets market elements previously missing. These EU initiatives will probably replace national regulations, which should provide greater certainty for the digital asset space in the present market. Until then, regulations (and troubles) around cryptocurrencies will remain on a state-by-state case.

Nowadays, there is a growing desire for autonomous financial systems in the form of cryptocurrency. European countries have supported this financial product, generating the need for legal protection and security. Therefore, there is still the urgent necessity to develop and improve the legal framework for regulating the circulation of cryptocurrency in Europe. The dissemination of legislative regulations on the functioning of cryptocurrency has been widely observed, even though a series of nations still demonstrate an evident inability to adequately and competently respond to the technological progress.

At the moment, none of the regulators of the EU has concretely embraced special rules related to the use of cryptocurrency. Taxation of transactions, for example, is carried out in accordance with the national legislation of the EU Member States. At the same time, they still consider cryptocurrency as an intangible asset or commodity, and not as currency or money. The term “virtual (digital) currency” is used in place of the word “cryptocurrency” by European regulators, even if, according to the European Central Bank (ECB), the latter definition is imperfect. Anyway, this does not contrast the need for an establishment of a proper legal framework for crimes committed through the use of cryptocurrencies.

Among other components, this explains the interest of the European Central Bank (ECB) in carrying out an analysis in face of its role as a catalyst for payment systems. The ECB defines virtual currencies schemes based on their characteristics. In particular, a virtual currency can be defined as a type of digital (unregulated) money, issued and controlled by its developers, and accepted between the members of a virtual community. Virtual currency schemes can be then classified into three types: the ones referring to closed virtual currency schemes (mostly used in online games); the ones having a unidirectional flow, so there is a conversion rate for purchasing the virtual currency; and the ones with a bidirectional flow, so with two exchange rates (buy and sell). The European Central Bank believes that the absence of a distinct legal framework leads to another important difference for which traditional financial actors are not involved. Since the issuer of the currency is usually a non-financial private company, financial sector regulations are not applicable. The point is that the link between virtual and traditional (fiat) currency is not regulated by the current law.

In July 2014, the European Banking Authority (EBA) issued its opinion on virtual currencies. The EBA highlighted a list of threats for virtual currency participants, existing financial institutions and regulators, concluding that only certain risks are able to be regulated, such as the risk of money laundering and financial crime, the contagion risk to conventional payment systems, and user-related information risks. The EBA has then recommended that already existing financial institutions should be mandate that virtual currencies exchanges comply with anti-money laundering and counter-terrorist financing requirements, rather than dealing with them. Two years later, the European Parliament adopted a resolution on virtual currencies (2016/2007(INI)) with the aim of implementing an approach for the legal regulation of virtual currencies at the EU level and identifying the problems associated with their use. However, since the technology itself is developing much faster than the legislator's regulatory attempts, detailed and accurate regulations will certainly require a very long process.

3.5. An American Comparison: the state of Wyoming

The economy of Wyoming (USA) has been always built on some of the oldest industries in human history, including agriculture and mining. Meanwhile, nowadays, the "cowboy state" has probably emerged as the most "crypto-friendly" American jurisdiction. Between 2018 and 2019, Wyoming has enacted 13 laws (so-called "blockchain bills") for which cryptocurrencies and tokens are recognized as money and assets, enabling decentralized economic operations to be conducted. These laws, in particular, addressed the treatment of digital assets in commercial law, and set the legal foundation for smart contracts.

Wyoming is also known as one of the "tax-friendly" US states. In fact, it detains lower overall taxation levels, and higher levels of economic freedom compared to every other state. The Limited Liability Company (LLC) type, for instance, was established in Wyoming before its spreading in the rest of the American soil. For these reasons, both cryptocurrency users and investors are so attracted to Wyoming. These changes enable the state banks to serve as custodians of digital assets, under a clear and unique legal framework. These banks also required the "Wyoming Division of Banking" (which is responsible for the regulation of banks in the same federal state) in order to issue a new kind of banking charter for those which mostly deal with digital assets. However, some people are worried that Wyoming's new charter will expose the national banking system to new risks.

According to the crypto laws of Wyoming, blockchain-based assets are categorized as three kinds of property assets: digital securities as investment contracts, digital consumer assets as utility tokens,

and virtual currencies as Bitcoin. Most of Wyoming's regulators have been supporting the idea of designing a "blockchain-friendly" legislation, enabling a new kind of banking category named "Special Purpose Depository Bank" (SPDB) by allowing banking services to blockchain-based businesses. The SPDB category represents the exemption of those utility tokens that are not marketed or promoted as investments and can be exchanged for goods and services. One of the most remarkable distinctions between SPDBs and traditional banks is the type of lending they engage in, since American federally chartered banks must comply with additional federal regulations as they typically lend out customer money and hold less in reserve than the customer initially deposited (also known as "fractional reserve banking").

These new crypto banks can operate as a national money transmitter without obtaining a license from all the states and can offer banking and qualified custody for digital assets for any company, integrating with federal payment systems. Yet, they can create new types of financial products for their customers, like cryptocurrency-backed debit cards or wealth management services. Ultimately, Wyoming's legislation means that DAOs (Decentralized Autonomous Organizations) are recognized as a legal form of business and that digital tokens are excluded from being considered a form of securities, enabling tokens to function as money.

In conclusion, the new 13 blockchain-enabled laws enacted within the Wyoming legislation can be summarized as follows:

I. The "Virtual Currency Exemption" (HB0019, 2018) modifies the already existing "Money Transmitter Act"[27] in order to exempt virtual currency transactions along with the requirements for a money transmitter license; and it defines virtual currency as a digital (or electronic) representation of value used as a medium of exchange, unit of account or store of value. It is not recognized as legal tender by the government of the United States.

II. The "Open Blockchain Tokens Exemption" (HB0070, 2018) defines "open blockchain token" as a digital unit created pursuant to a blockchain recorded transaction. The token is only exchangeable for goods, services or content.

[27] The US "Money Transmitter Act" provides for the licensing and the regulation of the businesses of transmitting money or credit for a fee or other consideration by the issuance of money orders, conferring powers and duties upon the Department of Banking and Securities.

III. The “Electronic Corporate Records” (HB0101) authorizes Wyoming corporations to use distributed and decentralized means for generating business records, as long as they are also convertible into written form.

IV. The “Limited Liability Companies – Series” (HB0126, 2018) authorizes a Limited Liability Company (LLC) to establish one or more designated members, managers, transferable interests or assets treated for certain purposes.

V. The “Property Taxation Digital Currencies” (SF0111, 2018), where virtual currency is any type of digital representation of value used for exchange, accounting or to store value, exempts virtual currencies from property taxation. It is not recognized as legal tender by the American government.

VI. According to the “Financial Technology Sandbox Act” (HB0057, 2019), the Banking Commissioner or the Secretary of State may allow specific regulations in order to let the testing of innovative financial products and services. The fintech sandbox is only available to Wyoming corporations.

VII. The “Wyoming Utility Token - Property Amendments” (HB0062, 2019) amends and clarifies the 2018 HB0070 concerning the exemption of open blockchain tokens from securities regulations.

VIII. The “Commercial Filing System” (HB0070, 2019) authorizes the Secretary of State to develop and implement a blockchain-based filing system for those firms otherwise required by law to be filed.

IX. The “Special Purpose Depository Institutions” (HB0074, 2019) recognizes that some financial institutions refuse to provide services to blockchain innovators or accept deposits in US currency obtained from the sale of virtual currency (or other assets). It produces a new form of financial institution to provide necessary financial services to blockchain innovators.

X. According to the “Special Electric Utility Agreements” (HB0113, 2019), an electric utility may negotiate with any customer having a projected electric usage greater than five megawatts for services provided under a tariff approved by the Public Service Commission.

XI. The “Corporate Stock Certificate Tokens” (HB0185, 2019) authorizes an entity to issue stock certificates in electronic form as a certificate token. It requires the network signature of two officers designated by the law or by the board of directors in order to validate the issuance of a certificate token.

XII. The “Banking Technology and Stock Revisions” (SF0028, 2019) authorizing banks to use electronic corporate records and issue any type of stock authorized for corporations under the existing laws; stockholder identity might be maintained using data addresses associate with a private key.

XIII. The “Digital Assets Existing Law” (SF0125, 2019) establishes the legal nature of digital assets within existing law, dividing them into 3 categories of intangible personal property and classifies them as: digital consumer assets, digital securities and virtual currencies. It authorizes banks to voluntarily provide custodial services for digital assets consistent with the act and the custodian requirements, defining “custodial services” as the safekeeping currency and digital assets through the exercise of fiduciary and trust powers as a custodian.

3.6. Final Proposal: a (late) “Sandbox-Approach” for EU

The European Commission recently (and finally) recognized the importance of legal certainty and the need for a clear regulatory framework in the areas pertaining to blockchain-based applications. The European Union strongly supports a pan-European framework, hoping to avoid legal and regulatory fragmentation. In order to increase investments and to ensure both consumer and investor protection, the EU Commission (on September 24, 2020) adopted a comprehensive package of legislative proposals for the regulation of crypto-assets, whose main objectives are: removing fragmentation in the Digital Single Market; adapting the EU regulatory framework to facilitate digital innovation; promoting data-driven innovation in finance by establishing a common financial data space; and addressing the challenges and risks associated with digital transformation. The basic goal is to create a legal structure for regulatory sandboxes of financial supervisors within the EU. A sandbox, in particular, is a facility that brings together regulators, firms, and tech experts for the evaluation of innovative solutions, trying to identify their opportunities and risks.

Besides, the Commission proposed a “pilot regime” for market infrastructures wishing to settle transactions of financial instruments in crypto-asset form. This pilot regime, specifically, allows for exemptions from existing rules and lets companies and legislators to test innovative solutions through the use of blockchains. For other crypto-assets that do not qualify as “financial instruments”, instead, the Commission proposed a new framework that would replace all the other EU laws as well as those national rules currently controlling such crypto-assets. The already mentioned Markets in Crypto-Assets Regulation (MiCA) will bear innovation, while preserving consumers and the integrity of cryptocurrency exchanges at the same time. The proposed regulation covers not only entities issuing crypto-assets, but also businesses providing services around crypto-assets and cryptocurrency exchanges.

In this regard, another fundamental milestone is represented by the European Blockchain Partnership (EBP), which is an initiative for developing an EU strategy on the blockchain technology. It establishes a blockchain infrastructure for public services, which main focus has been building the European Blockchain Services Infrastructure (EBSI). The Partnership firmly promotes interoperability and a broader deployment of blockchain-based techs, contributing to more efficient and more accessible cross-border government services across Europe. It also offers a regulatory environment in full compliance with EU laws, and it is planning the abovementioned pan-European regulatory sandbox in cooperation with the European Commission for use cases inside and outside the EBSI. The sandbox is expected to become operational between 2021 and 2022, though who knows how long it will really take.

CONCLUSION

Given the incredible expansion of blockchain and smart contracts during the recent past years, an analysis of their legal status (or legality) under the European legal framework appears almost necessary. In the absence of clear and applicable laws, this paper tried to focus on the major points of friction and divergences between the blockchain and the current rules in force within the European Union.

Once the basic principles of both blockchain and smart contracts phenomena has been explained, the aim of the paper was to frame these technologies in the European environment from a legal point of view. In particular, highlighting the most relevant shortcomings that the current EU regulatory framework still presents nowadays.

The potential of blockchain and smart contracts is enormous, but not free from criticalities. The inhomogeneity of the different regulations of the various EU Member States, indeed, does not present a promising future scenario, risking to exacerbate the already existing socio-economic disparities and increase the huge problem of the digital divide.

As reported in the very last paragraph of the dissertation, the EU commission has lately adopted a "sandbox-approach" for a "pan-European framework" with the hope of avoiding further legal fragmentation in this regard. However, the one proposed seems to be a belated attempt to remedy some regulatory gaps which are unlikely to be really filled. To this end, a solution could be represented by the formation of a univocal supranational regulatory framework across the EU, the implementation of which, however, is virtually a mirage as of now.

BIBLIOGRAPHY

CHAPTER 1

Alharby, Maher, Amjad Aldweesh, and Aad van Moorsel. "Blockchain-based smart contracts: A systematic mapping study of academic research (2018)." 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB). IEEE, 2018.

Di Pierro, Massimo. "What is the blockchain?." Computing in Science & Engineering 19.5 (2017): 92-95.

Leka, Elva, Besnik Selimi, and Luis Lamani. "Systematic literature review of blockchain applications: Smart contracts." 2019 International Conference on Information Technologies (InfoTech). IEEE, 2019.

Liu, Jing, and Zhentian Liu. "A survey on security verification of blockchain smart contracts." IEEE Access 7 (2019): 77894-77904.

Mohanta, Bhabendu Kumar, Soumyashree S. Panda, and Debasish Jena. "An overview of smart contract and use cases in blockchain technology." 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2018.

Wang, Shuai, et al. "Blockchain-enabled smart contracts: architecture, applications, and future trends." IEEE Transactions on Systems, Man, and Cybernetics: Systems 49.11 (2019): 2266-2277.

Watanabe, Hiroki, et al. "Blockchain contract: Securing a blockchain applied to smart contracts." 2016 IEEE international conference on consumer electronics (ICCE). IEEE, 2016.

CHAPTER 2

Catchlove, Paul. "Smart contracts: a new era of contract use." Available at SSRN 3090226 (2017).

De Filippi, Primavera, and Samer Hassan. "Blockchain technology as a regulatory technology: From code is law to law is code." arXiv preprint arXiv:1801.02507 (2018).

Jaccard, Gabriel. "Smart contracts and the role of law." Available at SSRN 3099885 (2018).

Lingwall, Jeff, and Ramya Mogallapu. "Should Code Be Law? Smart Contracts, Blockchain, and Boilerplate." UMKC L. Rev. 88 (2019): 285.

Radinger-Peer, Wolfgang, and Bernhard Kolm. "A blockchain-driven approach to fulfill the gdpr recording requirements." Blockchain and Distributed Ledger Technology Use Cases. Springer, Cham, 2020. 133-148.

Raskin, Max. "The law and legality of smart contracts." (2016).

Salmensuu, Cagla. "The general data protection regulation and the blockchains." Liikejuridiikka 1 (2018).

Schrepel, Thibault. "Is blockchain the death of antitrust law? The Blockchain Antitrust Paradox." Georgetown Law Technology Review/3 Geo. L. Tech. Rev 281 (2019).

Temte, Morgan N. "Blockchain challenges traditional contract law: Just how smart are smart contracts." Wyo. L. Rev. 19 (2019): 87.

Timsit, Tom & Herian, Robert. (2019). LEGAL AND REGULATORY FRAMEWORK OF BLOCKCHAINS AND SMART CONTRACTS.

Wright, Aaron, and Primavera De Filippi. "Decentralized blockchain technology and the rise of lex cryptographia." Available at SSRN 2580664 (2015).

Zetzsche, Dirk A., Ross P. Buckley, and Douglas W. Arner. "The distributed liability of distributed ledgers: Legal risks of blockchain." U. Ill. L. Rev. (2018): 1361.

CHAPTER 3

Allessie, David, et al. "Blockchain for digital government." Luxembourg: Publications Office of the European Union (2019).

Austria, KMU Forschung. "Advanced Technologies for Industry." (2021).

Chanson, Mathieu, Marten Risius, and Felix Wortmann. "Initial coin offerings (ICOs): An introduction to the novel funding mechanism based on blockchain technology." (2018).

Cvetkova, Irina. "Cryptocurrencies legal regulation." BRICS LJ 5 (2018): 128.

Ehmke, Cole, and Mariah Ehmke. "BLOCKCHAIN TECHNOLOGY APPLICATIONS IN THE WYOMING FOOD SYSTEM." Paper presented at the 22nd International Farm Management Association Congress. Vol. 3.

Ellul, Joshua, et al. "Regulating Blockchain, DLT and Smart Contracts: a technology regulator's perspective." ERA Forum. Vol. 21. No. 2. Springer Berlin Heidelberg, 2020.

Gouder, Nicky, and Luana Scicluna. "Malta: The Blockchain Island." Int'l Tax Rev. 29 (2018): 37.

Nascimento, Susana, et al. "Blockchain Now And Tomorrow-Assessing Multidimensional impacts of Distributed Ledger Technologies." European Union, Joint Research Centre. Luxembourg: Publications Office of the European Union. doi 10 (2019): 901029.

Nestertsova-Sobakar, Oleksandra, et al. "Legal approaches to the regulation of cryptocurrency and business ethics of ico in the European Union." Journal of Legal, Ethical and Regulatory Issues 22 (2019): 1-6.

Stacher, David. "Regulation of Initial Coin Offering (ICO)." Chair of Economic Theory Universität Basel. (2018).

Venegas, Percy. "Initial coin offering (ICO) risk, value and cost in blockchain trustless crypto markets." Value and Cost in Blockchain Trustless Crypto Markets (August 1, 2017) (2017).

SITOGRAPHY

CHAPTER 1

https://101blockchains.com/blockchain-adoption-challenges/

https://101blockchains.com/introduction-to-blockchain-features/

https://builtin.com/blockchain

https://builtin.com/blockchain/blockchain-applications

https://corporatefinanceinstitute.com/resources/knowledge/deals/smart-contract/

https://medium.com/coreledger/what-are-smart-contracts-a-breakdown-for-beginners-92ac68ebdbeb

https://www.computerworld.com/article/3412140/whats-a-smart-contract-and-how-does-it-work.html

https://www.devteam.space/blog/5-best-smart-contract-platforms/

https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain

https://www.financemagnates.com/fintech/blockchain-is-it-all-hype/

https://www.ibm.com/topics/smart-contracts#:~:text=Smart%20contracts%20are%20simply%20programs,intermediary's%20involvement%20or%20time%20loss

https://www.infosys.com/insights/digital-future/smart-contracts.html

https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology

https://www.sipotra.it/wp-content/uploads/2018/07/The-Impact-of-Blockchain-Technology-on-Finance-A-Catalyst-for-Change.pdf

CHAPTER 2

https://lawgazette.com.sg/feature/legal-risks-beneath-blockchain-enabled-smart-contracts/

https://media.consensys.net/report-the-legal-and-regulatory-framework-of-blockchains-and-smart-contracts-8f397eaf0b1f

https://ndlsjet.com/antitrust-in-the-blockchain-era-2/

https://op.europa.eu/en/browse-by-subject?p_p_id=eu_europa_publications_portlet_search_executor_SearchExecutorPortlet_INSTANCE_wEsJBR19pzHZ&p_p_lifecycle=1&p_p_state=normal&facet.eurovoc.subject=c_ab84e157&facet.collection=EULex%2CEUPub%2CEUWebPage%2CEUSummariesOfLegislation&language=en&startRow=1&resultsPerPage=10&selectedSubjectId=c_ab84e157&SEARCH_TYPE=BROWSE_BY_SUBJECT

https://siriuslegaladvocaten.be/en/the-legal-challenges-of-blockchain-and-smart-contracts/

https://www.bdpinternational.com/blog/gdpr-blockchain-at-the-intersection-of-data-privacy-and-technology

https://www.competitionpolicyinternational.com/is-blockchain-the-real-antitrust-game-changer/

https://www.cyberlaws.it/2018/blockchain-technology-challenges-legal-issues/

https://www.dlapiper.com/en/oman/insights/publications/2017/06/blockchain-background-challenges-legal-issues/

https://www.law.ox.ac.uk/business-law-blog/blog/2019/12/blockchain-and-human-rights-utopia-or-dystopia-or-both

https://www.oulu.fi/blogs/node/194666

https://www.twobirds.com/en/news/articles/2018/global/blockchain-technology-and-competition-law-issues-to-be-considered

CHAPTER 3

https://blockchaintechnology-news.com/2021/03/cryptocurrency-concerns-vs-regulations-in-europe-a-guide/

https://blockchaintechnology-news.com/2021/03/cryptocurrency-concerns-vs-regulations-in-europe-a-guide/

https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2021/04/27/Distributed+Ledger+Technologies+Shaping+the+Future+of+Digital+Governments

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591

https://financemalta.org/app/uploads/2019/10/Malta-Destination-Blockchain-Island.pdf

https://medium.com/the-capital/launching-an-ico-in-europe-your-legal-obligations-c73b3c49efc6

https://sites.les.univr.it/eisic/wp-content/uploads/2019/11/33-Sabbagh-1.pdf

https://vladanlausevic.medium.com/wyoming-as-a-blockchain-and-crypto-friendly-state-a9d02746ec9f

https://www.cnbc.com/2020/09/24/eu-valdis-dombrovskis.html

https://www.icmagroup.org/assets/documents/Regulatory/Quarterly_Reports/Articles/QR-article-DLT-related-legislation-and-regulatory-frameworks-130120.pdf

https://www.law.ox.ac.uk/business-law-blog/blog/2020/11/dlt-pilot-regime-eu-sandbox-last

https://www.marketwatch.com/story/how-wyoming-became-the-promised-land-for-bitcoin-investors-11619201182

https://www.whitecase.com/publications/alert/update-status-initial-coin-offerings-europe