universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

“The implementation of the protection of the human rights in the framework of the block-chain technology and crypto-currencies operations”

verfasst von / submitted by

ANDREA EMANUELE

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Arts (MA)

Wien, 2018 / Vienna 2018

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	A 992 884
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Master of Arts in Human Rights
Betreut von / Supervisor:	Univ.-Prof. Dr. Nikolaus Forgó

SPECIAL THANKS

Al Professor Nowak, a Marijana, a Georges e a Sabine, per il loro supporto, la loro professionalità, le loro esperienze e la loro passione.
Ai miei compagni di classe, per i dibattiti, le esperienze che hanno deciso di condividere, gli scambi di opinione, le risate insieme e per avermi fatto apprezzare la bellezza della diversità!
Alla mia famiglia, per aver creduto sempre in me e per non avermi mai fatto mancare il loro supporto emotivo, economico e affettivo.
A Monica. Nonostante tutte le difficoltà che abbiamo incontrato, mi ha accompagnato in questo viaggio di due anni, non facendomi mancare mai il suo amore.
A Ruggero, per l'amicizia sincera.
A mio Nonno Mario, venuto a mancare all'inizio di questo Master. Non c'è stato un giorno da quanto te ne sei andato in cui non ho avvertito la tua presenza in tutto ciò che facevo. Continua a guardarmi e guidarmi dovunque tu sia.

To Professor Nowak, Marijana, Georges and Sabine, for their support, their professionalism, their experiences and their passion.
To my classmates, for the debates, the experiences they have shared, the exchanges of opinion, for the laughs together and for making me appreciate the beauty of being part of the human rights' world!
To my family, for having always believed in me and for never making me miss their emotional, economic and emotional support.
To Monica. Despite all the difficulties we encountered, she accompanied me in this two-year journey, never making me miss her love.
To Ruggero, for his sincere friendship!
To my grandfather Mario, who passed away at the beginning of this Master. There has not been a day since you left in which I didn't feel your presence in everything I did. Keep looking at me and guide me, wherever you are.

ACKOWLEDGEMENTS

Trying to relate the economic field of expertise to Human Rights is undoubtedly not an easy task. Both the fields seem so unrelated between them others, and most of the time a reconciliation seems impossible. Nevertheless, this context never scared me, rather it motivated me more!
Before doing this master, I already completed another master in international commercial law and my personal belief is that the global human rights situation could be sensibly improved by making specific economic investments, aiming to transfer not only moneys, but a bigger and solid know-how, in order to reduce the gap between richest and poorest countries.

Before choosing the topic of this thesis, I was hence looking for a topic which could have been related to my beliefs. Then, one day, I was talking with a friend of mine who actively works within the Bitcoin and cryptocurrencies field. He was very enthusiast of his job, but at the same time he showed me his worries about the future. “As long as there won’t be regulations, I will always perceive myself as a precarious worker”. From that moment, I started to ask to myself if the situation of Human Rights within the Bitcoin Network was sufficiently protected or if it was necessary to make some step further. I started reading a lot of very technical papers, full of mathematical formulas, related to Bitcoin, its functioning, and its potential uses outside the economical field.

Now that my thesis is done, I feel really grateful to have chosen such a difficult and theorical topic, but with such very interesting applications in the next future. Moreover, I am developing a project with some friends, which aims to build an electronic platform in which people can give money directly to small NGO’s working in humanitarian emergencies contexts. By using the block-chain technology, the donors can choose to which project devolve their money and, in every single moment, they can check how those moneys are used and spent.

LIST OF ABBREVIATIONS

"AEPD"	Agencia Española de Protección de Datos
"AML	Anti Money-Laundering
"ATMs	Automated Teller Machine
"CEO"	Chief Executive Officer
"CFR"	Charter of Fundamental Rights
"DEA"	Drug Enforcement Administration
"DPD"	Data Protection Directive
"DPO"	Data Protection Officer
"EBA"	European Banking Authority
"EC"	European Commission
"ECHR"	European Convention on Human Rights
"ECtHR"	European Court of Human Rights
"ECJ"	European Court of Justice
"EJF"	Environmental Justice Foundation
"EPD"	e-Privacy Directive
"Epr"	ePrivacy regulation
"EU"	European Union
"FATF"	Financial Action Task Force
"GDPR"	General Data Protection Regulation
"IT"	Information Technology
"KYC"	Know Your Customer
"POW	Proof Of Work
"U.S"	United States
"WFP"	World Food Program

TABLE OF CONTENTS

INTRODUCTION

In recent years, new technologies have produced inventions that, in most cases, have helped to sensibly improve the quality of life of individuals. These new technologies do not only refer to hi-tech inventions. Some of these innovations, on the contrary, have contributed to improve aspects of individuals' life which for long time were considered "not perfectible". One of these technological improvements embraces the sphere of decentralized payments, using virtual currencies and the innovative "block-chain" technology. Among these virtual currencies, or cryptocurrencies, the most famous example are bitcoins. Initially, the use of this form of payment was adopted only by an inner circle of experts and, most of the times, not for legal purposes. In these past years, especially in 2017, these crypto-currencies and the block-chain technology have attracted a growing number. *De facto*, something that only a few years ago was considered as a visionary concept, used by some niche and smart experts, became a concrete and existing reality. The number of investors and workers within this alternative form of payments is growing day by day.

Until now a univocal political answer toward this new technological phenomenon wasn't given by the Central Authorities. Some countries were more open and tolerant; others, instead, choose to adopt restrictive policies. The fact is that this technology embraces a whole bunch of rights, which require appropriate legal protection in order to be legitimately exercised. Very often, due the pseudoanonimity granted to the users within the Bitcoin network, bitcoin payments are used for illicit purposes, such as for money laundering or for financing terrorism. In other cases, users steal bitcoins from other users' 'account' and it is impossible to obtain a legal protection in this sense. It follows that this phenomenon cannot be underestimated anymore by the International and the National authorities. The ongoing lack of regulation can no longer be tolerated, because it would entail (to) a growing uncertainty for all the people involved in these crypto-operations and, in the worst cases, to open acts of discrimination between workers. The aim of this research will be, moving from the existing legal framework within the European Union, to go further in order to find new approaches which States can uses in order to cope with the Bitcoin phenomenon and with the human rights violations associated to it.

METHODOLOGY

Bitcoin is a world-wide phenomenon which opens up to issues on a global scale. In order to assess what are the major problematics faced by individuals in exercising their rights, the present work will tackle these issues in a twofold manner. The first one consists in the analysis of the human rights related to this new form of technology, by considering only the European legal framework. More specifically, the analysis will focus on the legal discipline on the right to privacy, right to property and right to work, given by the ECHR and EU Charter of Fundamental Rights. This analysis has two main purposes: on one hand, to give a general idea about what these rights consist of, what characteristics they have and how they can be fully enjoyed by individuals. On the other hand, the analysis aims to describe what duties the states have towards their own citizens in guaranteeing their full and legitimate enjoyment and under what circumstances states are entitled to limit these same rights. Subsequently, the work will take into account the situations in which users and workers are not enable to the exercise their rights due the main features of Bitcoin network and blockchain technology. These same features will play a key role when the major problems encountered by the States will be examined. Lastly, the work will conclude by making a comparative analysis amongst the different European States approaches, in order to evaluate whether they are able to cope with the human rights violations and, at the same time, to respect the obligations deriving from the European conventions.

ASSUMPTION/HYPOTHESIS

In talking with some friends who are actively working in the Bitcoin sector, I noticed that they were complaining about the lack of sufficient legal remedies applicable to their jobs and their careers. I started asking myself whether the human rights involved in the Bitcoin network are sufficiently protected by the European Convention or if the States should make further steps in order to guarantee an adequate protection to those who have chosen to invest and work within this field.

RESEARCH QUESTION(S)

Due the non-governmental nature of the network, it follows that the role of central authorities, for what concern in particular the obligation to protect human rights, may be more marginal than in the past. The research questions which I want to address in this work will be:

- Who is the subject entitled to implement the protection of the human rights connected to the Bitcoin operations and to block-chain?
- Is the same Bitcoin users' community entitled to grant the enjoyment of certain human rights or, rather, should be the central governments to introduce specific standards to govern the legal aspects of this phenomenon?
- If yes, how?
- Or, again, is a legal implementation really necessary?

CHAPTER I
THE BLOCK-CHAIN TECHNOLOGY AND BITCOIN

1.1 Bitcoin and block-chain: a background history.

The concept of "Bitcoin" was born at the end of 2008. An unknown person (or a group of people, there is an ongoing debate about it) - under the pseudonym of Satoshi Nakamoto - published a research paper called "*Bitcoin: A Peer-to-Peer Electronic Cash System*".[1] This paper, spread through a cryptography mailing list,[2] described a new generation of money and of payment system, based on some innovative pillars:

- a version of electronic cash, the Bitcoin;
- the possibility of sending payments directly and instantaneously from one party to another;
- the prevention from the double-spending through the creation of a peer-to-peer [3] network;
- no mint or other trusted parties;
- the creation of a timestamp server in which registering all the operations, forming a sort of "chain" of transactions;
- granting to the participants of these transactions a complete anonymity;
- new coins are made utilizing the Hashcash style proof-to-work.[4]

What happened after the spread of this paper was astounding. In less than one year, the Internet community took the protocol described within Nakamoto's paper and created what is known now-adays as Bitcoin network.[5] Moving from these very humble premises, essentially based on creating something out of nothing, Bitcoin network grew at an exponential rate.[6] In 2017 bitcoin market

1 S. Nakamoto, "*Bitcoin: A Peer-to-Peer Electronic Cash System",* available from https://bitcoin.org/bitcoin.pdf (accessed the 18th April 2018)

2 http://www.metzdowd.com/mailman/listinfo/cryptography, accessed the 18th April 2018

3 In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client.

4 The Hashcash system, invented by Adam Black in 1997, is a proof-of-work algorithm, which has been used as a denial-of-service counter measure technique in a number of systems. A hashcash stamp constitutes a proof-of-work which takes a parameterizable amount of work to compute for the sender. The recipient (and indeed anyone as it is publicly auditable) can verify received hashcash stamps efficiently. For further information, see http://www.hashcash.org (accessed 18 April 2018)

5 T. B.Jenssen, "Why Bitcoins Have Value, and Why Governments Are Sceptical?", Master's thesis, University of Oslo, 14 May 2014, p.1, available at https://www.duo.uio.no/bit-stream/handle/10852/40966/Jenssen-Torbjorn-Bull.pdf?sequence=7&isAllowed=y , (accessed the 18 April 2018)

6 Ibidem

capitalisation has seen the highest peak since its creation, when over 300 billion dollars were reached at the end of December 2017. [7]

Historically speaking, Bitcoin wasn't the first form of cryptocurrencies. The idea of making untraceable payments through the use of a blind signature technology was already introduced at the beginning of the 80's, with a paper signed by David Chaum.[8] In this paper, Chaum introduced the idea of a new kind of cryptography, able to allow to an automated payments systems to have the following features: prevent "*third parties to determine payee, time or amount of payments made by an individual*"; enable "*individuals to provide proof of payments, or to determine the identity of the payee under exceptional circumstances*"; the *ability to stop use of payment media reported stolen*.[9] In this paper, Chaum proposed also one of the key aspects of today's Bitcoin technology: a two keys digital signature system, a "private key" and a "public (crypted) key", which allows the anonymity of the users. Then, in 1990, Chaum went further with his idea, proposing the creation of an Untraceable Electronic Cash (eCash system),[10] also introducing the concept of preventing the "double-spending". As the first cryptocurrency, the eCash system was available via various banks and smart cards in various countries, such as the United States and Finland. It slowly evolved into the current form of cryptocurrencies used nowadays, with many refinements by various software developers over the last 20 years.[11]

Digital gold currencies, instead, came into the limelight between 1999 and the early 2000's. The major part of these new forms of electronic moneys, based on ounces of gold, were stored at the bullion and storage fees were charged.[12] Most of these currencies ended up very soon in the graveyard due to both compliance issues or regulatory breaches. The most known of these currencies was e-Gold, which was considered as the pioneer for Internet Payments. The latter, in fact, was the first successful online micropayment system; it has led to many new techniques and methods for e-commerce which, few years later, became widely used under other aspects.[13] The most innovative techniques introduced by e-Gold were the possibility of making payments over a Secure Socket Layer-encrypted connection and offering an application programming interface to enable

7 https://blockchain.info/it/charts/market-cap?timespan=1year, accessed 18 April 2018

8 D.Chaum, *Blind Signatures for Untraceable Payments*, In: Chaum D., Rivest R.L., Sherman A.T. (eds) *Advances in Cryptology*, Boston, MA, 1983, pp.199-203, available at https://www.chaum.com/publications/Chaum-blind-signatures.PDF (accessed the 18 April 2018)

9 Ibid.

10 D. Chaum, Achieving Electronic Privacy, in *Scientific American*, vol. 267, iss. 2, 1992, pp. 96-101

11 L.P. Nian, D.Lee K. Chuen, 'Introduction to Bitcoin', in D.L.K. Chuen, *"Handbook of Digital Currency"*, Academic Press, 29th April 2015, pp. 5-30, p. 9

12 Ibidem

13 Ibidem.

other website to build services using e-gold's transaction system.[14] Despite these innovative introductions, this system failed when they had to face suspicious transaction reporting requirements and, furthermore, hackers' attacks and Internet frauds.

At the onset of the global financial crisis in 2008, interest on cryptocurrencies was revived. It was argued[15] that the cryptocurrencies have the potential to counter a few problems commonly associated with the fiat currency system. It was mooted the concept of 'bit gold', to be mined and bit recorded on a digital register. What Szabo proposed was a "simple" protocol which requires participants to spend resources to mine the digital gold (or bit gold) in order to be rewarded and, during this process, validate the public digital register. The loss of trust in the fiat currency, exacerbated during the economic crisis of 2008, has brought the consumers' attention to cryptocurrencies for those who wanted to hedge their position with a currency that has a finite supply.[16] Cryptocurrencies were perceived to be as a debt-free currency with a constant growth rate. The use of cryptocurrencies as a safe haven and an alternative asset class was demonstrated in 2013 Cypriot property-related bank crisis: on that occasion, a 6.75% levy was imposed on bank deposit up to € 100k, and 9.9% for even larger deposits.[17] With their confidence in traditional banking system heavily shaken, an increasing number of investors decided to convert their flat money into a more stable alternative: bitcoins.

Cryptocurrency usage has exploded since Bitcoin's release. Though exact active currency numbers fluctuate and individual currencies' values are highly volatile, the overall market value of all active cryptocurrencies is generally trending upward.[18] At any given time, hundreds of cryptocurrencies trade actively. Despite the creation of an incredible amount of digital currencies after bitcoin's great success (approximately there are 1414 different cryptocurrencies)[19], Bitcoin still remains the most well-known and reliable currency of its type.

14 Ibidem.

15 N. Szabo, "Bit gold", 27 December 2008, available from http://unenumerated.blogspot.com/2005/12/bit-gold.html (accessed 23rd April 2018)

16 L.P. Nian, D.Lee K. Chuen, 'Introduction to Bitcoin', in D.L.K. Chuen, *"Handbook of Digital Currency"*, Academic Press, 29th April 2015, pp. 5-30, p. 10

17 G. Koumoullis, "Revisiting the 2013 banking crisis", CyprusMail Online, 22 October 2017, available from http://cyprus-mail.com/2017/10/22/revisiting-2013-banking-crisis/ (accessed 23rd April 2018)

18 B. Martucci, "*What Is Cryptocurrency – How It Works, History & Bitcoin Alternatives*", in Money Crashers, available at https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/ (accessed the 23 April 2018)

19 P. Magliocco, "Quante monete come i bitcoin esistono?", La Stampa -Economia, 13 January 2018, available at http://www.lastampa.it/2018/01/13/economia/quanti-monete-come-i-bitcoin-esistono-UWXjyrQxYw37VNH7A97yqI/pagina.html, (accessed 23 april 2018)

1.2 What are bitcoins?

Bitcoin is a cryptocurrency, which is a subset of what is generally known as a digital currency. An important distinction has to be stressed in this introductory part. The term *digital* is very often used interchangeably with the term *virtual*, when describing currencies based on an electronic value.[20] This is a very common terminology misuse. The term virtual, in fact, has a negative connotation, since it describes something that only "seems real" but not exactly "real".[21] When we refer to a currency stored in a "digital" or in an "electronic" register, these currencies described as "virtual" are, instead, very real, in the sense that they exist.[22] Thus, the correct (and more neutral) terminology generally preferred is digital currencies. Another small, but important, clarification has to be made when talking about Bitcoin. At is core, Bitcoin is just a digital public ledger used to enforce and operate private property rights of the virtual unit bitcoin. When it is written with the upper B, Bitcoin defines the technology and the network; on the other hand, bitcoin (with lower case b) defines the digital unites transferred within the network.

The Bitcoin protocol, like the HTML for webpages, regulates how peers in the network can interact.[23] Bitcoin protocol uses an open-source software, which means that can be downloaded by anyone, and the system runs on a decentralized peer-to peer network. The main purpose of the protocol is to enable people to transfer electronic cash directly between each other within the same network, without resorting to trusted third parties. Traditionally, in fact, trusted third parties, such as the banks, have operated payment systems, *de facto* enabling complete strangers to interact economically through the exchange of IOU's, [24] with claims on assets or national fiat currencies. The Bitcoin protocol, on the other hand, was born as an alternative payment form to the fiat currencies markets.

When it comes to fiat currency, we refer to the legal tender whose value is backed by the government that issued it. The word "*fiat*" comes from the Latin and it means literally "let it be done".[25] When it is associated to the word "money", it refers to a currency which has to be authorized and backed by a central, trusted, authority. These currencies can take the form of physical currency

20 L.P. Nian, D.Lee K. Chuen, 'Introduction to Bitcoin', in D.L.K. Chuen, *"Handbook of Digital Currency"*, Academic Press, 29th April 2015, pp. 5-30, p. 6

21 Ibid.

22 Ibid.

23 T. B.Jenssen, "Why Bitcoins Have Value, and Why Governments Are Sceptical?", Master's thesis, University of Oslo, 14 May 2014, p.16, available at https://www.duo.uio.no/bitstream/handle/10852/40966/Jenssen-Torbjorn-Bull.pdf?sequence=7&isAllowed=y , (accessed the 25 April 2018)

24 Business Dictionary, http://www.businessdictionary.com/definition/IOU.html , (accessed the 25 April 2018)

25 https://www.vocabulary.com/dictionary/fiat , accessed the 26th April 2018

(for instance, the U.S. dollar is a fiat money, as are the Euros and many other major world currencies), or it can be represented electronically, such as with bank credit. The prices of goods denominated in state money would be determined by the ratio of required work in production to the work required to obtain the money from the state. The government controls the supply and citizens can pay their taxes with it. When a State issuing money accepts the same money in discharge of taxes, the state's flexibility in spending increases. Although new fiat money could, theoretically speaking, enter the economy through government spending, it was correctly noted that "*most countries operate under institutional structures, in which money issuance passes through the Central Banks*".[26] The fiat currencies are hence created in a credit way, through the central banks' balance sheets expansion. Cryptocurrencies such as bitcoins, instead, are not "legal tender" and are not backed by a central government or bank, due their decentralized and global nature. Their form is more like a bank credit, but without the bank (in that it is represented digitally, but not backed by a bank or government). An algorithm controls the supply and you can't pay your taxes with it. Except for these differences, there are no intrinsic variations between fiat and digital currencies. Both fiat currencies and cryptocurrencies can be called money or currency, both are mediums of exchange that are used to store and transfer value, both can be used to purchases goods and services, both have their value governed by supply, demand, work, scarcity, and other economic factors, both have their value affected by the quality of the system surrounding it, both can be traded on exchanges, etc.

Since there is no central authority that is entitled to issue currencies, a question that could legitimately arise is how bitcoins are created and by whom? The answer to this question was provided by the same Nakamoto's paper, when it says that is the same Bitcoin network which provides to create new coins, "*adding an incentive for nodes*[27] *to support the network and provides a way to initially distribute coins into circulation, since there is no central authority to issue them*".[28] Bitcoins can be created by anyone with the right hardware through a process called *mining*. During this process, similar to a continuous lottery draw, the nodes of the network receive a bitcoin prize every time they solve a specific mathematical problem their computers. When they solve the problem, they generate a new block. Once this block is registered within the Bitcoin Network, the nodes

26 T. B.Jenssen, "Why Bitcoins Have Value, and Why Governments Are Sceptical?", Master's thesis, University of Oslo, 14 May 2014, p.16, available at https://www.duo.uio.no/bitstream/handle/10852/40966/Jenssen-Torbjorn-Bull.pdf?sequence=7&isAllowed=y , (accessed the 25 April 2018)

27 A node can be any active electronic device, including a computer, phone or even a printer, as long as it is connected to the internet and as such has an IP address. The role of a node is to support the network by maintaining a copy of a blockchain and, in some cases, to process transactions.

28 S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, p. 4, par. 6, available at https://bitcoin.org/bitcoin.pdf, , accessed the 28th April 2018.

receive the 'prize' for their work.[29] The difficulty of this process varies with the growth of the network. The prize for creating a block is automatically adjusted so that every four years of network work will create half of the bitcoins generated in the previous four years. In the first 4 years (from January 2009 to 2012) almost 10,5 million of bitcoins were issued. Every four years this sum will be halved. It was esteemed that, in the following four years (from 2013 to 2017) the amount of bitcoin created was to 5,250,000. Nowadays, since the huge growing of the network, the currencies created will be around then to 2,625,000 for the next for years, and so on. Because of the currency's high value, one bitcoin is dividable to a maximum of eight decimals, allowing you to send someone just 0.00000001 Bitcoin.[30] Like gold, Bitcoin is also scarce: its supply is limited. The total sum of bitcoins will never exceed 20.999.839.77085749. This total amount of 21 million is the overall amount of all the bitcoins which will be created and distributed among the network, which is expected to happen around the year 2040. After the creation of this total amount of 21 million, *mining* will be self-limited and won't be no longer be possible.

A final clarification about bitcoins' value has to be made. How is it possible to establish a value to this cryptocurrency, since is not possible to bind it to a central authority able to give this currency a value stability? The answer to this question is 'rather' simple and it lies in basic economic laws. There are four characteristics thanks which it is possible to give a value to each good: scarcity, utility, supply and demand.[31] If something is both rare (scarce) and useful (utility) it must have value and demand a specific price, with all other things being equal. A classic example of this, is gold: its value is so expensive because it is rare, hard to find and limited in supply. In addition, consumers benefit directly from its use (utility).[32] At the same time, bitcoins have value for their usefulness and for the fact that there is a limited amount. Like gold, Bitcoin is perfectly fungible (one Bitcoin is similar to another, like the atoms of gold are all the same), it is divisible and easily verifiable (via the Blockchain).[33] Bitcoins, moreover, have other desirable properties. They are fast, borderless and decentralised with the potential to change the financial world.[34] Not

29 "How are new bitcoins created?", available at https://en.bitcoin.it/wiki/Help:FAQ (accessed the 28th April 2018)

30 The different units in which bitcoin can be sub-divided are: 1 BTC = 1 bitcoin; 0.01 BTC = 1 CBTC = 1 centbitcoin (also called bitcent); 0.001 BTC = 1 mBTC = 1 millibitcoin (also called mbit, millibit or millbit); 0.000 001 BTC = 1 μBTC = 1 microbitcoin (also called ubit or microbit); 0.000 000 01 BTC = 1 satoshi (as a form of tribute to the creator, Satoshi Nakamoto).

31 L. Visser, "Why does Bitcoin have value and how is the price determined?", LUNO, 15 March 2017, available from https://www.luno.com/blog/en/post/how-bitcoin-price-determined, (accessed the 29 April 2018)

32 K.S. Taylor, "Theories of Value", in K.S. Taylor "*Human Society and the Global Economy",* 2001, Online Economic textbooks, Suny-Oswego, Department of Economics, Chapter 6.

33 L. Visser, "Why does Bitcoin have value and how is the price determined?", LUNO, 15 March 2017, available from https://www.luno.com/blog/en/post/how-bitcoin-price-determined, (accessed the 29 April 2018)

34 Ibidem

only does it currently have value as a payment system, but also as an asset class (a store of wealth). Bitcoin has also an undeniable utility when compared to other, newer cryptocurrencies. There is simply no other digital currency that is as widely used and integrated at this point in time. Through network effects, we're starting to see its exponential growth, which creates value as more and more people start using Bitcoin and more merchants accepting it as a means of payment.[35] Today, there are already thousands of merchants around the world accepting Bitcoin as a means of payment, thus proving the growing usefulness of it.

Bitcoins' price is always going up or down and is the result of supply and demand law,[36] just like the price of gold. As soon as bitcoin payments will be accepted by more and more sellers of goods and services, the value of the bitcoins will stabilize. In the next paragraph will be deepened the functioning of the Bitcoin network in all its aspects.

1.3 How Bitcoin works?

The purpose of this paragraph will be to explain how Bitcoin network concretely works and how the operations with bitcoins are realized. There are two ways in which it is possible to obtain bitcoins: the first one is by buying them in the exchange stores or from another bitcoins' possessor. The second way is through a process called *mining*, through which it is the same Bitcoin network that reward the miners with new bitcoins.

1.3.1 Buying and storing bitcoins

Typically, a user who wishes to spend bitcoins obtains it by exchanging real world currencies for bitcoins.[37] Usually, bitcoins may be obtained in the Bitcoin exchange shops or in the exchange or vending machine or simply from another person. Bitcoin vending machines, often called "ATMs" are the most convenient way to buy bitcoins. A person can simply insert cash into a machine to obtain bitcoin instantly.[38] On this point, a first question may legitimately arise. As it was said in

35 Ibidem

36 Demand and supply represent, in the classical economic theory, the relation which determines the price of a commodity. This relationship is thought to be the driving force in a free market. As demand for an item increases, prices rise. When manufacturers respond to the price increase by producing a larger supply of that item, this increases competition and drives the price down. Modern economic theory proposes that many other factors affect price, including government regulations, monopolies, and modern techniques of marketing and advertising. (http://www.dictionary.com/browse/supply-and-demand, accessed the 1st may 2018).

37 L.P. Nian, D.Lee K. Chuen, 'Introduction to Bitcoin', in D.L.K. Chuen, *"Handbook of Digital Currency"*, Academic Press, 29th April 2015, pp. 5-30, p. 18

38 B. Ulm," *Bitcoin ATMs boom: new locations"*, Cointelegraph, 28 July 2014, available from https://cointelegraph.com/news/bitcoin-atms-boom-new-locations, (accessed the 3rd may 2018)

the previous paragraph, in the Bitcoin network there isn't a central authority which issues the currencies. Therefore, there are not bank accounts. Where is it possible hence storing bitcoins and authorizing operations?

Bitcoins can be sent by and received on a Bitcoin *"wallet"*. These wallets can be created through mobile apps, computer software or services provider specifically designated for that. Concretely speaking, a Bitcoin wallet is a program with which is possible to send and receive bitcoins, store bitcoins and monitor bitcoin balances.[39] As well as there are programs to manage emails, the bitcoin wallets are necessary in order to manage bitcoins. The wallet generates an address, comparable to a bank account number, through which is possible to identify the user's wallet, and from which the user can start to receive payments. The important exception is that a Bitcoin address is a unique alphanumeric sequence of characters, encrypted in a way to grant the absolute privacy and anonymity to the respective users.

In order to spend the money associated to an account, a pair of keys, one public and one private, is needed. Like a normal password is required to gain access to a personal bank account, so is the private key. A private key is just a very long string of numbers and letters which is used to access to Bitcoin wallet and sign transactions. The Private Key is used to mathematically derive the Public Key, which is then transformed – through an hash function- to produce the address that other people can see and to which it is possible transfer bitcoin from one user to another.[40] The pair of keys associated to a "Bitcoin account" are different but generated in a way which makes them mathematically related. This becomes crucial at the time of authorizing a transaction.

A bitcoin transaction happens when a peer in the network wants to transfer some bitcoin from his/her wallet to another peer in the network's wallet. All he/she has to do is to broadcast a message like "send 5 bitcoins from my wallet to *subject x*'s wallet" to the network. The computer participating in the work of maintaining the ledger, the so-called "nodes", after receiving the message, will update their copy of the ledger and pass along the transaction message.[41] In order to verify if the request of sending five bitcoins is authentic, the nodes use a "digital signing scheme". When the private key of the transferring user and the transaction message are combined in a mathematical

39 O. Beigel, *"What is a Bitcoin Wallet – Bitcoin Whiteboard Tuesday",* 99 Bitcoins, 4 July 2018, available at https://99bitcoins.com/what-is-bitcoin-wallet-bwbt-3/, (accessed the 1st may 2018)

40 L. Di," *Why Do I Need a Public and Private Key on the Blockchain*?", WeTrust, 30 January 2017, available at https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76, (accessed the 1st May 2018)

41 UNODC, "Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies", June 2014, p. 32, available at http://www.imolin.org/pdf/FULL10-UNODCVirtualCurrencies_final.pdf, (accessed the 2nd May 2018)

function, a unique signature is generated. To verify this signature, and therefore the validity of the transaction request, the signature is put into a verification together with the message and the transferring user's public key. The "relation" between the public and the private key will allow to conclude whether the user private key was used to generated the signature or not. The uniqueness of the signatures is an important feature in the Bitcoin Protocol, since it ensures that signatures cannot be copied and reused by others. As a result of this 'bind' between message and signature, past transactions cannot be changed without invalidating the signature. Daniel Kraft has pointed out that one of the major difficulties is "*to ensure that the entire peer-to-peer network reaches a consensus about the current state of the ledger. In particular, the owner of an address may create two mutually conflicting transactions, spending the same balance twice to different recipients. This may lead to some parts of the network considering the first recipient to be the new owner of the coins and rejecting the second transaction, while the other part of the network has it the other way around. This is called double spending*."[42] From this point of view, Bitcoin is revolutionary because it is able to solve the double-spending problem without needing a third trusted party. By maintaining a ledger of balances, whose control is entrusted to the entire network, Bitcoin has solved this problem instead of relying on a single, trusted, third party to manage the ledger. The whole Bitcoin network constantly keeps track of bitcoin balances in the public ledger called "block-chain". New transactions are checked against the block-chain, making sure that a certain amount of bitcoin has not been already spent, solving the double-spending problem at its roots.

1.3.2 The block-chain

The block-chain is a publicly accessible authoritative ledger of all the bitcoin transactions ever processed. This ledger allows anyone using Bitcoin software to verify the validity of a transaction. It is important to stress the difference between block-chain and transactions chain. The latter shows the transaction history of all the bitcoins ever created. The ownership of a certain number of bitcoins (or fractions of bitcoins) is therefore validated through the verification of links to previous transactions.[43] The validity of any transaction of bitcoins relies on the whole chain of transaction with those bitcoins leading up to the transaction in question. The verification process has to be

42 In computer science, the double spending problem refers to the problem that digital money could be spent more than once by the same person, in favour of two distinct subjects. Without a trusted third-party intermediary to ensure the control, this can easily happen. D. Kraft, "Difficulty Control for Blockchain-Based Consensus Systems". Master Thesis, University of Graz, 18 March 2015, p. 1 available at https://www.weusecoins.com/assets/pdf/library/University%20of%20Graz%20Blockchain%20Difficulty%20Control.pdf (accessed the 1 May 2018)

43 There are two types of transactions: the incoming transactions to a peer are called "inputs"; the new transactions authorized by the same peer are called "outputs". In order to verify these new transactions. nodes will have to check that the inputs actually belong to the transferring peer.

done only once, when the Bitcoin wallet software is used for the first time. In that occasion, the whole transaction of all bitcoins is downloaded and checked.

When transactions are broadcasted to the network, nodes collect unverified transactions, by gathering them into blocks. A node, after verifying the entire blockchain, collects the newly generated (unconfirmed) transactions and suggests to the network what the next block should be.[44] There is a possibility for multiple nodes to create such blocks at the same time; therefore, in order to validate a block, the node must contain a solution to a very special math problem.[45] The activity of validation of a block is called *mining*, and it will be deepened in the next paragraph. Once a block is created and it is broadcasted to the network and subsequently accepted, it is possible to start working on the next block. Every new block in the chain confirms the integrity of the previous one, all the way back to the first block called the "genesis block". [46]

The whole network relies hence on a shared *consensus* mechanism. Whenever a transaction enters into the Peer to peer network, the nodes validate this transaction. If (all) the nodes agree on its legitimacy, they confirm the transaction and their decision is laid down in a block. In this way the latest block added to the 'chain' maintains a shared, agreed-upon view of the current state of the Block-chain.[47] If a node manages to find a new block, it is allowed to award itself a certain number of bitcoins. This creates strong economic incentives for the network as a whole to find a consensus.[48] However, this does not mean that the block-chain is unalterable. The controlling parties which set up the block- chain – ranging from citizens to public or private organizations – can decide to alter the history of the block-chain, introducing altered blocks which counterfeited, irregular, or duplicated transactions. This could happen if attackers were able to control 51% of the whole computing power in the system before they can generate the longest block chain by constructing fraudulent transaction records. This possibility known in the Bitcoin community as 51% attack is a major concern of Bitcoin system security, although it seems unlikely that a single node could control more than half of the system's computing power. Some observers argued that 51% attacks are not incentive-compatible, because attackers will act to their own detriment. [49]

44 N.D. Bashar& D.L.K.Chuen, "Bitcoin Minin technology", in *Handbook of Digital Currency* Academic Press, 29th April 2015, Ch.3, pp. 45-65, p. 49-50

45 Ibidem

46 Ibidem.

47 V. Buterin, *Ethereum White Paper: A next-generation smart contract and decentralized application platform*., 2014 (Retrieved from https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, accessed the 1st May 2018)).

48 D. Kraft, 'Difficulty control for blockchain-based consensus systems', in *Peer-to-Peer Networking and Applications*, Vol.9, n.2, 2016, pp.397-413

49 M.Vasek, M.Thornton, T.Moore, "Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem", in *Lecture Notes in Computer Science* (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol.8438, 2014, pp.57-71.

1.3.3 Mining to create new bitcoins

The other way in which bitcoins may be obtained by users it through *mining*. As we saw in the previous paragraphs, the limit of bitcoins is designed to 21 million of units. These bitcoins are generated by the same Bitcoin network as a compensation form for the activity of mining.

In what *mining* consists? During this activity miners, who are Bitcoin users running software on specialized hardware, contribute in maintaining the blockchain by adding newly validated blocks of bitcoins transactions to it.[50] Only legitimate transactions can be recorded within the block-chain. This recording is the result of a computationally very intensive verification process. As a reward for dedicating their computing power to the network, miners are rewarded with newly mined bitcoins and transaction fees.[51] The miners with high computing power are most likely to solve a block first; however, the difficulty of mining increases as more blocks are solved.

In order to solve these mathematic problems, computers use a cryptographic hash to estimate an output until it is below the target value (given by the "bits" header field), and the only way to predict the output is by random guesses. The first node who solves the block broadcasts it to the network and gets accepted as the next block in the chain. To solve this mathematical problem, the Bitcoin Protocol uses a "Proof of Work" (POW) scheme to create what Nakamoto defined as "distributed timestamp server".[52] The name Proof of Work describes the work of letting a computer use computational skills and energy to guess the problem. It is computationally costly and time-consuming for users to generate this data, but they are rewarded for attempting to do this with new bitcoins. POW computation is a random process and is estimated on trial and error basis.[53] Although a node can be lucky and guess the solution at the first trial, it will take the network approximately ten minutes to come up with the solution. It is the same protocol, moreover, who regulates the necessary time to generate a new block.

There are three ways in which mining can be made: solo mining, mining contracts, and mining pools.[54]

50 "How Bitcoin Mining Works", available at https://www.bitcoinmining.com/ (accessed the 1st May 2018)

51 N.D. Bashar& D.L.K.Chuen, "Bitcoin Minin technology", in *Handbook of Digital Currency* Academic Press, 29th April 2015, Ch.3, pp. 45-65

52 S. Nakamoto, https://bitcoin.org/bitcoin.pdf, accessed the 3rd May 2018

53 To get on with the growth of computing power in the network, the system recalibrates the difficulty of the mathematical problems every two weeks. See, N.D. Bashar& D.L.K.Chuen, "Bitcoin Minin technology", in *Handbook of Digital Currency* Academic Press, 29th April 2015, Ch.3, pp. 45-65, p. 47

54 Ibidem

1. In solo mining, miners compute hash is individually and the reward on solving a block will be paid entirely to the owner of the hashing computer. The chances of earning new bitcoins are very low since even a very well-equipped solo miner would take an average of three months to earn any reward. Mining process is random and memoryless. So, if the miner does not solve a block by the end of these three months, then he or she is not any close to solving a block than he or she was at the beginning of the period.[55] Before venturing into this form of mining, each solo miner must always take into consideration factors such as cost of mining equipment, the electricity cost and the difficulty to find a hash below a given target, which may seriously affect their earnings expectations;

2. A second for of mining are the so-called "mining contracts". The latter are suitable for those who would like to invest in bitcoin mining without the hassle of either managing the hardware or operating the software necessary for mining.[56] These contracts provide mining services, with specific performances to be fulfilled in a determined amount of time. Mining shares are also available, that is, shares of hardware of large-scale mining centres. This is a process known as "Cloud mining".[57] "Cloud mining" means using shared processing power run from remote data centres. A user only needs a home computer for communication purposes, optional local bitcoin wallets, and the like. As it is described by Bashar and Chuen in their 'Handbook of Digital Currencies', [58] there are three types of mining contract options:

    - Hosted mining, when a user leases a mining machine that is hosted by the provider. It contributes some systematic risk to the network. For this type of mining, when a substantial amount of computing power is consolidated in large hosting providers, there is a possibility for the provider to control the network to a certain extent.

    - Virtual hosted mining: in which a user can create a virtual private server to mine bitcoins and also install his or her own mining software.

    - Leased hashing power: when a user can lease an amount of hashing power without having a dedicated physical or virtual computer from a data centre that is formed by a

55 , N.D. Bashar& D.L.K.Chuen, "Bitcoin Minin technology", in *Handbook of Digital Currency* Academic Press, 29th April 2015, Ch.3, pp. 45-65, p. 53

56 N.D. Bashar& D.L.K.Chuen, "Bitcoin Minin technology", in *Handbook of Digital Currency* Academic Press, 29th April 2015, Ch.3, pp. 45-65, p. 54

57 Ibidem

58 N.D. Bashar& D.L.K.Chuen, "Bitcoin Minin technology", in *Handbook of Digital Currency* Academic Press, 29th April 2015, Ch.3, pp. 45-65, p.57

group of bitcoin miners. The data centre then takes a share from any newly mined bitcoins.[59]

3. Mining pools are groups formed by many miners that collectively use all their resources and mine together, aiming to generate combined higher hashing power. Being a part of a mining pool increases the probability of quickly mining a block, as the probability of solving a block is in direct proportion to the computational resources. Bitcoin mining is made less risky by such pools. The reward is divided among the participants based on their level of contribution. The income earned per miner is steady but lesser, because the transaction fee is not cashed out and additional fee is charged by the pool operator to compensate for the incurred expenses.[60]

1.4 The criticisms associated to Bitcoin and Block-chain technology.

Since the beginning of its theorization and subsequent creation, Bitcoin has always been seen with a negative connotation, attracting very strong oppositions both by the conservative side of the economists and by legal and political experts. The purpose of this chapter is to analyse - with a purely informative end and in an absolutely impartial manner- which are (or were) the most common criticisms associated to the whole Bitcoin phenomenon. In order to realize this, jointly to a copious literature, I also conducted an interview with the former director of the Faculty of Economy of the University Tor Vergata in Rome, Professor Michele Bagella, who is strongly against Bitcoin technology. The same approach will be used in the next chapter, in which will be deepened Bitcoin positive aspects by using, even in this circumstance, the literature and an interview with an academic representative, Professor Ferdinando Ametrano, who is instead fully in favour of the use of this technology.

Undoubtedly, a first condemnation toward Bitcoin has to be traced back to the lack of a central control within the Network. As Bagella said, "*while in the traditional fiat currencies systems, the control starts by the central Bank (or by a central Authority) and it develops through the lines of control supplied by the same central bank, this doesn't happen within the Bitcoin network*."[61] Because of the lack of regulations and oversight, cryptocurrencies and virtual currencies lack con-

59 Ibidem.

60 N.D. Bashar& D.L.K.Chuen, "Bitcoin Minin technology", in *Handbook of Digital Currency* Academic Press, 29th April 2015, Ch.3, pp. 45-65, p.58

61 Interview with Michele Bagella, Rome, 6th April 2018., Annex 1

sumers' protection. As a "digital representation of value", bitcoins are obviously exposed to operational risk; due to hardware malfunction or software collapse, bitcoins stored in a personal wallet or in external accounts may vanish completely. In case of fraud there is no form of legal protection or jurisdiction that a user can invoke, so it is impossible for any form of reimbursement. For the same reason, in absence of regulation, fraudulent events or closing activity of exchange platforms or wallet providers can cancel customers' bitcoin balances. This lack of control embraces not only the 'security' of the investments of the people involved within the network, but it also affects the convenience in promoting the use of a certain means of exchange as an integral part of commercial strategies.

This lack of control embraces not only the 'security' of the investments of the people involved within the network, but it also affects the convenience in promoting the use of a certain means of exchange as an integral part of commercial strategies. When the critical balance between competition and cooperation holds and if consumers' security is not reduced, alternative payment instruments and procedures can foster the market's efficiency. On the contrary, in a system in which there are no authorities to guarantee this security, the market is in a state of perennial uncertainty and risk. Jointly, merchants and payment service providers could adopt inadequate and unsound behaviours, so that consumers might not correctly perceive hidden risks related to unregulated peer-to-peer payment schemes.[62] Due its lack of a central authority, able to issue the currency, it was also stated [63] that the whole Bitcoin network relies its functioning on the so-called "Ponzi scheme", in which users' investments can be re-payed only with the funds invested by new users that join the scheme, and so it implodes when it is no longer possible to find new investments.[64] The correct operation of the payment system has always been considered a function of public interest, not a profit maximizing activity.

A second economic criticism[65] stems exactly from here. A private money scheme could have a negative impact on the payments' ecosystem, whenever firewalls do not exist and many matters still remain unresolved, also due to the unclear functional, institutional and legal definition of virtual currencies. Furthermore, as a 'community-driven project', Bitcoin continues to undergo

62 G. Bonaiuti, Economic Issues on M-Payments and Bitcoin, in G. Gimigliano "*Bitcoin and Mobile Payments*, London, Palgraves Studies in Financial Services Technology, 2016, pp. 27-51. p. 46

63 M. Bartoletti, B. Pes, S. Serusi, *Data mining for detecting Bitcoin Ponzi schemes*, 1st March 2018, available at https://arxiv-org.uaccess.univie.ac.at/pdf/1803.00646.pdf, accessed the 5 may 2018

64 M. Artzrouni, "The mathematics of Ponzi schemes," in *Mathematical Social Sciences*, 2009, vol. 58, no. 2, pp. 190–201.

65 G. Bonaiuti, Economic Issues on M-Payments and Bitcoin, in G. Gimigliano "*Bitcoin and Mobile Payments*, London, Palgraves Studies in Financial Services Technology, 2016, pp. 27-51

changes as software developers improve it and change the software with consensus of network users.[66] At the same time, the price of bitcoins continues to fluctuate, as external events may affect the price. Some significant price changes are said to resemble a traditional 'speculative bubble', which may occur when optimistic media coverage attract an increasing number of unwise investors, just for the prospect of easy earnings.[67] This make also difficult to determine how good bitcoins are as a store of value,[68] and merchants accepting bitcoins often convert them out into fiat currency very quickly. The risk of incautious investments must be considered in conjunction with the exchange rates. Each investor has to choose the appropriate moment in which changing its bitcoins, following the market trends. This, for the unwary, it can be risky and unproductive, and it seems that "*only those who are ready to accept the high level of risks related to the volatility and the value of the bitcoins can withstand*".[69]

With the pseudoanonimity, granted by the encrypted Bitcoin addresses, and ease of payment without the duty of declaring to a central authority the sums transferred, it is no wonder that international governments are concerned with the use of Bitcoin in incentivizing criminal activities. Indeed, one of the most well-known illegal uses of bitcoin was for purchasing drugs and weapons (and in the worst cases, even for hiring hitmen) on the Deep-web. When it comes to Deep-web, or Dark-web, it refers to a distinct network supporting cryptographically hidden sites. In this way Deep Web came into existence, attracting growing amounts of criminals seeking the advantages of moving their activities to the Dark-web. A quantitative research on the Deep-web, operated in 2016 by Daniel Moore and Thomas Rid, has indicated that more than fifty percent of all content on the Dark Web is illegal.[70.]

The most known examples of Dark-website in which bitcoin were used for illegal activities was "Silk Road". On January 2011, an anonymous user - who was Silk Road's founder, Ross Ulbricht - on a forum of the website www. shroomery.org [71] unveiled "Silk Road", which was described as

66 L.P. Nian, D.Lee K. Chuen, 'Introduction to Bitcoin', in D.L.K. Chuen, *"Handbook of Digital Currency"*, Academic Press, 29th April 2015, pp. 5-30, p. 24

67 F. Salmon, The Bitcoin Bubble and the Future of Currency, 3 April 2013, available at https://medium.com/@felixsalmon/the-bitcoin-bubble-and-the-future-of-currency-2b5ef79482cb, (accessed the 6th may 2018)

68 D.G. Baur, H. KiHoon, A. D. Lee, 'Bitcoin: Medium of exchange or speculative assets?', in *Journal of International Financial Markets, Institutions & Money*, available at https://www-sciencedirect-com.uaccess.univie.ac.at/science/article/pii/S1042443117300720, accessed the 6th May 2018

69 Interview with Michele Bagella, Rome, 6th April 2018.

70 D.Moore & T. Rid, 'Cryptopolitik and the Darknet', in *Survival, Global Politics and Strategy*, vol. 58, iss.1, 2016, p. 7-38.

71 Shroomery.org is a website in which users describe their experiences with psychedelic mushrooms. On this point, see P.H. O'Neill, *The Definitive History of Silk Road*, The Daily Dot, 11 October 2013, available at https://www.dailydot.com/crime/silk-road-drug-ross-ulbright-dread-pirate-roberts-history/, (accessed the 6th may 2018)

a "*Tor* [72] *hidden service that claims to allow anyone to buy and sell anything online anonymously*". 'Silk Road' was defined as '*a certifiable one-stop shop for illegal drugs that represented the most brazen attempt to peddle drugs online that we have ever seen*'.[73] It has revolutionised Internet drug sourcing and has been described as an '*eBay for Drugs*".[74] Despite this was not the first existing online market for illicit substances, it was the first one to combine Tor and Bitcoin technology for its services. Users have had the chance of buying and selling a vast series of illegal products, from drugs to counterfeit documents. Between 2012 and 2013 Silk Road rapidly expanded; during this period of time it was possible to arrest only few people until when, in October 2013, the Dark-site was shut down due a long undercover investigation made by DEA,[75] and its creator Ross Ulbricht was arrested. The Government of the United States has estimated that, during its short lifespan, Silk Road has generated $214 million of gross income.[76] In May 2015, Ulbricht was sentenced to life in prison by the Court of New York,[77] and this sentence was confirmed two years later in appeal.[78]

Another major concern regarding Bitcoin is its potential use to launder money and finance terrorist activities. Money laundering is not a new criminal phenomenon. As E. Savona said, money laundering '*is a constantly changing criminal phenomenon, with updated modus operandi and evolving business models*'.[79] Traditionally, the laundering of crime money is facilitated by money mules, offshore accounts, or luxuries products, i.e. art, houses, boats, or a combination of those. This process of laundering is typically segmented in three stages: *placement*, *layering* and *integration*.[80] It is crucial to identify the money laundering risks associated with any emerging payment or value

72 Tor, acronym for The Onion Router, is a type of internet browser created to ensure secure government communications for the U.S Navy. When browsing or transmitting data, Tor encrypts and sends the information through layers of randomized relay nodes located all over the world, protecting the individual user from having their browsing linked to their IP address, making it difficult for governments or law-enforcers to identify users.

73 U.S Senator C. Shumer said this in June 2011. For further information see NBC New York, *"Schumer pushes to shut down online drug marketplace*", NBC New York, 5 June 2011, available at https://www.nbcnewyork.com/news/local/Schumer-Calls-on-Feds-to-Shut-Down-Online-Drug-Marketplace-123187958.html, (accessed the 8th may 2018).

74 M. Barratt, 'Letters to the editor Silk Road: Ebay for drugs', in *Addiction*, 2012, vol. 107, pp. 683–684.

75 C. Di Piero, 'Deciphering Cryptocurrency: Shining A Light On The Deep Dark Web', in *University Of Illinois Law Review*, 2017, iss.3, pp. 1267-1298

76 K. Soska & N. Christin, *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem*, available at https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf, accessed the 8th may 2018

77 S. Thielman, *Silk Road operator Ross Ulbricht sentenced to life in prison*, The Guardian, 29 May 2015, available at https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced (accessed the 8th May 2018)

78 United States v. Ulbricht, available at https://www.pbwt.com/content/uploads/2017/05/15-1815_opn.pdf, accessed the 8th May 2018.

79 E. Savona, 'Organised crime numbers', in *Global Crime*, vol. 15, 2014, pp. 1–9.

80 K.K.R. Choo, "New payment methods: a review of 2010-2012 FATF mutual evaluation reports", in *Computer & Security*, vol.36, 2013, pp. 12–26. The author describes how these three phases find their fulfilment. In the *placement* stage, the money launderer introduces corruption proceeds into the financial system or acquires nonmonetary instruments of value such as art and antiques, precious metals, and cryptocurrencies and virtual currencies. After the corruption proceeds have entered the financial system or used to acquire nonmonetary instruments of value, the money launderer may engage in a series of transactions to distance the funds from their source. In this (*layering*) stage, the funds might be channelled through the purchase of cryptocurrencies and virtual currencies or by transferring money electronically through a series of cryptocurrencies and virtual currency accounts. The money launderer might also seek to disguise the transfers as payments for goods or services, thus giving them a legitimate appearance. In the *integration* phase, disguised funds (cleaned money) would appear to have been legally earned, and it is extremely difficult to discern between legal wealth and illegal wealth at this stage

transfer mechanism or product since it is only through understanding those risks that they can be effectively mitigated. It is for this reason that the Financial Action Task Force (FATF) publishes typology reports which detail both particular money laundering processes identified over a given period and specific risk factors associated with those typologies.[81] Today, so called new-payment methods are becoming a more important factor in actual money laundering schemes. Amongst the categories of new payments methods, a specific mention is given to cryptocurrencies. In this context, in fact, cryptocurrencies such bitcoins offer an accessible facility for the transfer of value across international borders without reliance on the (heavily regulated) traditional financial and credit institutions. The level of anonymity associated to Bitcoin explains why this currency has become so popular in illegal activities. The total system however – from a criminal perspective - has one 'downside'. Due to the blockchain concept, all historic information on any bitcoin address and transactional information is just one mouse-click away for law enforcement authorities.

According to the FATF report, "*these decentralised systems are particularly vulnerable to anonymity risks*".[82] By design, in fact, in the Bitcoin network the addresses, which function as accounts, have no names or other customer identification attached. Moreover the whole system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity.[83] There is no central oversight body, and no anti money-laundering (AML) software currently available to monitor and identify suspicious transaction patterns. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect).[84] It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems, such as PayPal.[85] As a result of these risks, many governments are putting in place systems to ensure that Anti-Money

81 In Financial Action Task Force– FATF- *'Guidance for a risk-based approach to virtual currencies*', Paris, June 2015, p.4, available at http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf (accessed the 9th may 2018), the attention is concentrated on exchangers, where "*convertible virtual currencies activities intersect with regulated fiat currency financial system".*

82 Financial Action Task Force– FATF- *'Guidance for a risk-based approach to virtual currencies*', Paris, June 2014, p.9, available at http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf , (accessed the 2nd may 2018)

83 N. Hajdarbegovic, "Financial Watchdog FATF Examines Risks of Digital Currencies", Coindesk, 30 June 2014, available at https://www.coindesk.com/financial-watchdog-fatf-examines-risks-digital-currencies/ (accessed the 2nd May 2018); Financial Action Task Force– FATF- *'Guidance for a risk-based approach to virtual currencies*', Paris, June 2014, p.9, available at http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf , (accessed the 2nd may 2018)

84 B. El Nakib, "What is Bitcoins, How It Works? The Financial Action Task Force Issues Bitcoin Guidelines, Warns about Money Laundering", Compliance Alert, 15 February 2016, available at http://calert.info/details.php?id=781, (accessed the 2nd May 2018); Financial Action Task Force– FATF- *'Guidance for a risk-based approach to virtual currencies*', Paris, June 2014, p.9, available at http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf , (accessed the 2nd may 2018)

85 Financial Action Task Force– FATF- *'Guidance for a risk-based approach to virtual currencies*', Paris, June 2014, p.9, available at http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf , (accessed the 2nd may 2018)

Laundering and Know Your Customer (KYC) regulations are in place to identify individuals carrying out Bitcoin transactions. These regulations are often aimed at exchanges or financial institutions that facilitate Bitcoin transactions. AML regulations are enacted to prevent the conversion of money obtained from illegal activities into legitimate assets.[86] KYC regulations are intended to ensure that financial institutions are aware of the identities of their customers to ensure that unauthorized individuals (such as minors or criminals) don't have access to certain services.

1.5 The positive aspects and the potential benefits of Bitcoin and block-chain technology.

Next to the negative aspects associable to the whole Bitcoin technology, there are also many positive elements which are directly connected to this innovative concept. The first aspect which has to be considered lies in the cultural importance of the whole technology theorized by Nakamoto. Indeed, in order to fully understand the correct functioning of this technology, and therefore of the mathematical functions that distinguish it, the level of knowledge of the people involved must be very high. If, on one hand, buying and selling bitcoin through the exchange store or via specific phone apps may seem easy, on the other hand the comprehension of the subtleties and the functioning of the network, without a deep and constant study, appears very difficult. Furthermore, the costs to access to this technology are very high, especially for what concerns the machines and computers necessary for the *mining* activity. Nevertheless, these two issues, the high level of knowledge of the technology and the costs of access for mining, are the driving forces on which the whole network relies.

The proof of that has been, until now, the high level of efficiency of this network which, despite the lack of a centralized control, was granted by the same users operating within the network. How is this possible? According to Ferdinando Ametrano, one of the strongest Bitcoin phenomenon academic supporters in Italy, we are facing more a "*cultural paradigm shift*"[87], instead of a mere technological innovation. This cultural shift has introduced the already mentioned concept of "shared consensus" which, *de facto*, translates into a widespread control. Everyone is interested in improving the functioning of the network. If the network is constantly implemented, everyone benefits from it. Moreover, this mechanism is able to guarantee also a widespread security, both from outside and inside the network. If someone will try to manipulate or to counterfeit the way

86 A. Norry, "Bitcoin and Money Laundering: Complete Guide to Worldwide Regulations", BlockOnomi, 2 July 2018, available at https://blockonomi.com/bitcoin-money-laundering/ (accessed 2nd May 2018)

87 Interview with Ferdinando Ametrano, Milan, 24th April 2018.

in which Bitcoin works, more specifically the transactions within the block-chain, the joint control of all the user is able to prevent this opportunity.

From an economic point of view, Bitcoin has introduced important features for what concern the promotion of local economies and, most importantly, the implementation of economic freedom. Most of the times, financial services are overpriced and the whole financial system is too expensive to be accessible to the majority of investors. By promoting community forms of commerce, localism contributes to incentive consumption within a group of independent resellers or within a specific geographical area for job creation and improvement of business conditions.[88] The joint use with a mobile device fosters Bitcoin's diffusion among non-banked or underbanked people that frequently transfer small amounts of money, even across countries.[89] In this sense the Bitcoin scheme can also help financial inclusion. The lack of regulation, the absence both of third parties and of exchange rate fees lessen the total cost of payments. Usually, foreign remittances are charged for a fee of 5 % on average, when money transfer operators' services are used, while the average voluntary fee applied in the bitcoin scheme is about 1 %.[90]

The huge advantage of transferring value through the internet without passing through a trusted third party (and without paying transaction fees) has encouraged the usage of bitcoin, implementing the concept of economic freedom. This category of motivation refers to the individual economic convenience and has to be distinctly considered for demand and offer sides. On one hand, individual users of this new payment scheme (consumers and merchants) are pushed by a reduction in costs and time requested in transferring money, easy access to the payment system and the global reachability. On the other hand, firms offering bitcoin correlated services—or virtual currencies payment products and services- are, according to Financial Action Task Force's (FATF) definition, more interested in easier way to make business, selling everything related to the innovative process.

Economic libertarian users prefer a medium of exchange not fostered by the state, and, in particular, a payment system where banks or other financial intermediaries are not engaged at all. This position, certainly a minority, can be considered as a consequence of the general criticism, exac-

88 L.P.Nian & D. Lee K. Chuen, ' Introduction to Bitcoin', in David Lee Kuo Chuen, H*andbook of Digital Currencies,* Elseviert Inc., 2015, pp. 6-30

89 G. Bonaiuti, Economic Issues on M-Payments and Bitcoin, in G. Gimigliano "*Bitcoin and Mobile Payments,* London, Palgraves Studies in Financial Services Technology, 2016, p. 43

90 G. Bonaiuti, 'Economic Issues on M-Payments and Bitcoin', in G. Gimigliano (eds) *Bitcoin and Mobile Payments*., Palgrave Studies in Financial Services Technology, Palgrave Macmillan, London, 2016, pp.27-51

erbated by the global economic crisis of 2008, towards banking and finance operators as representatives of a disruptive financial world. Since the beginning of the crisis, there was a growing disillusionment about the high pay of CEOs and bankers, as well as the widespread belief of traditional banks too big to fail. With high debt and quantitative easing, there is a great discomfort with the economic uncertainty. It must however be stressed that "*this is not an anarcho-capitalist fight against the system. It is not necessarily a violent revolution, this is a liberal revolution*"[91]

Another factor which has to be cited when it comes to Bitcoin's positive aspects is environmentalism. There are growing ecology concerns and doubts whether if the point of maximum extraction of natural resources was reached. A major value of these alternative currencies lies in the amount of energy necessary to produce them, which is largely inferior to the energy and resources necessary to produce the flat money currently used. A recent study has suggested that, at current prices, that Bitcoin miners will consume an estimated 8.27 terawatt-hours per year.[92] Despite this might seem a lot, it's actually less than an eighth of what U.S. data centres use, and only about 0.21 percent of total U.S. consumption.[93] It also compares favourably to the currencies and commodities that bitcoin could help replace: Global production of cash and coins consumes an estimated 11 terawatt-hours per year,[94] while gold mining burns the equivalent of 132 terawatt-hours. And that doesn't include armoured trucks, bank vaults, security systems and such. So, in the right context, bitcoin is "positively green".

Many other sectors consider as the true innovation of Bitcoin its record system, that is the cryptographic method to build the public ledger, the blockchain. Traditional banking operators have tried to compete on this aspect, offering easier access to payment instruments, like various solutions of home and phone banking. Furthermore, further competitive pressure could come from the expected rapid growth in instant payments, also coming from non-bank payment service providers with a bitcoin system. Many authors have published articles listing a huge variety of benefits which might be accomplished by using the blockchain technology. Basic benefits are undoubtedly related to improved data integrity. As we have seen in chapter 1.3.3, blockchain system guarantees an almost absolute irrefutability of transactions registered within the ledger. Due this almost impossibility or

91 Interview with Ferdinando Ametrano, Milan, 24th April 2018., Annex 2

92 M. Bevand, 'Electricity consumption of Bitcoin: a market-based and technical analysis', available at http://blog.zorinaq.com/bitcoin-electricity-consumption/, accessed the 11th may 2018

93 E. Ou, "No, bitcoin won't boil the Oceans", Bloomber.com, 7 December 2017, available at https://www.bloomberg.com/view/articles/2017-12-07/bitcoin-is-greener-than-its-critics-think, (accessed the 11th may 2018)

94 H.McCook, 'Under the Microscope: The Real Costs of a Dollar', CoinDesk, 5 July 2014, available from https://www.coindesk.com/microscope-real-costs-dollar/, accessed 11th may 2018

extreme difficulty in changing or removing the data recorded, Blockchain may affect economic, social and political outcomes by many direct and indirect pathways. The first of blockchain's direct benefits is the potentiality to reduce or eliminate integrity violations such as fraud and corruption.[95] This can happen thanks to incontrovertible veracity of the information. Information stored in a system correspond to what is being represented in reality, due the need for consensus voting when transacting. The security is created by having distributed ledgers which hard to manipulate, since hacks or unauthorized changes are difficult to made without being unnoticed, as information are open. The consequence of this distributed control is a higher data quality.[96]

1.6. Conclusions

Conclusively, it is undeniable that nowadays we are facing a new paradigm within the global economy with the rising of the new cryptocurrencies. Despite it might be very easy to create a cryptocurrency as an alternative currency for free, it was stressed that "*most of these new creations cease their circulation within a short amount of time because, with many alternative currencies in competition, only a few will be globally adopted, such Bitcoin, reach a sufficient scale or find a suitable market."*[97] Until the dominance of national currencies will not be less, many of these cryptocurrencies will cease their circulation for various reasons – from progress in overcoming technology to more stringent regulations or insufficient demand. On the other hand, it is obvious that the aspects related to the decentralization of the control within these new markets is generating growing concerns for the world governments.

The economic incentives among the users has fostered the resilience of Bitcoin as a network and as a currency. Perhaps it is still too early to draw definitive conclusions about the validity of the system but, for sure, the decentralized nature of payments is convincing more and more users, disappointed by the central authorities, in believing in this new cultural paradigm.

95 N. Kshetri, "Will blockchain emerge as a tool to break the poverty chain in the Global South?", in *Third World Quarterly,* 2017, vol. 38, iss.8, pp. 1710-1732.

96 D. & A. Tapscott, '*The Impact of the Blockchain Goes Beyond Financial Services*', Harvard Business Review, 10 May 2016, available at https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services, accessed the 12th may 2018

97 L.P. Nian, D.Lee K. Chuen, 'Introduction to Bitcoin', in D.L.K. Chuen, *"Handbook of Digital Currency"*, Academic Press, 29th April 2015, pp. 5-30, p. 8

CHAPTER II

- THE HUMAN RIGHTS INVOLVED IN THE BITCOIN NETWORK AND THE MAJOR ISSUES ASSOCIATED TO THEIR ENJOYMENT-

Introduction

As it was stated in the previous chapter, when it comes to Bitcoin we not only refer to a technological and economic innovation, but also to a real cultural paradigm shift. In the course of history, when new technological and cultural innovations occurred, the surrounding society used to adapt herself more or less rapidly to these same innovations, and it has changed and evolved with them. Like any cultural revolution, also the Bitcoin phenomenon embraces a whole series of aspects, from the socio-cultural to the political, passing through a technological and economical innovation, and eventually the normative framework. *De facto,* the whole Bitcoin phenomenon can shift the discourse about human rights' protection to a new, more complicated level.

Due the non-governmental nature of the network, it follows that the role of central authorities, for what concern in particular the obligation to protect human rights, could be more marginal than in the past. The objective of this chapter will be hence to focus, through a specific legal analysis, on the existing legal framework in Europe toward specific human rights and which are the States' obligations. The attention will be given to three specific human rights: right to privacy, right to property and right to work. Indeed, it has to be recalled that there are many other human rights which may have been deepen in this work, given the numerous aspects embraced by the whole phenomenon. Concrete examples in this sense are the right to a fair trial – both for those who want to resort to a court in case of violation of their right within the Bitcoin network, as well as in the case of perpetration of an offense using Bitcoin - or the prohibition of discrimination - which finds a concrete application with some overly restrictive policies against bitcoin owners adopted by some states.

The choice of these three specific rights lies not only in the numerous questions that arose in an initial study of the Bitcoin phenomenon, but also in the legitimate concerns and doubts that have

been told to me by people directly involved in this sector. I found them the most likely to be violated or not to receive a possible legal protection, because of the blurred boundaries between legality and illegality within the Bitcoin network. The legal analysis carried out in this chapter will be restricted only to the European framework. In order to analyse the current definition and protection of these human rights, will be considered the European Convention on Human Rights (ECHR) and its protocols, on one hand, and the Charter of Fundamental Rights of the European Union. In particular, the study will focus on the core elements of each right, in order to evaluate their 'extension' and the situations in which these rights can be legally limited by the central authorities. This will introduce to the States obligations descending from the ratification of these Conventions, also by considering the case law of both the ECtHR and the ECJ for each right, which could be useful in order to define the boundaries in which States are obliged to carry out their legal actions. This will allow not only to understand to what extent the powers of governments are effective, but above all it provides a clear idea of what are the additional steps must be taken with respect to the current legislative framework in order to cover all the possible legal gaps. The analysis will also take into account the conspicuous case law both of the ECtHR and of the ECJ, in order to 'build' a solid jurisprudential background that will form the basis for the various approaches that States should have towards bitcoin users' human rights violations.

The second part of this chapter will focus then on the major difficulties related to the enjoyment and the implementation of the afore mentioned human rights within the Bitcoin network. In order to reach this purpose, it will be firstly operated an identification of the numerous rights holders being part of the Bitcoin Network. Subsequently, the analysis will shift to the practical issues users are facing in the enjoyment of their human rights. Finally, the work will deepen the major difficulties faced by the States –in this work identified as duty-bearers- in providing an adequate protection towards the users. This will we be helpful in order to introduce the final part of this work, focused on the European States approaches and if they are human rights oriented or not.

PART 1

– THE HUMAN RIGHTS INVOLVED IN BITCOIN OPERATIONS AND BLOCK-CHAIN TECHNOLOGY –A SURVEY ON THE CURRENT LEGAL EUROPEAN REGULATION

2.1. The Right to privacy within the European Legal Framework.

Europe is generally seen to have a strong and rather detailed regulatory environment for what concerns right to privacy and data protection. The protection of these rights is deemed necessary and it is specified both in the ECHR and in the EU Charter of Fundamental Rights. At the same time, within the EU, there are two main directives which shape the regulatory environment for privacy and data protection: the e-Privacy Directive (EPD)[98] and the recently adopted the General Data Protection Regulation (GDPR), which has repealed the former Data Protection Directive (DPD). Concerning the respect of private life, articles 8 of ECHR and 7 of the EU Charter are pretty identical. Nevertheless, the EU Charter went further by introducing - with article 8 - the protection of personal data. In order to give a detailed and specific legal analysis, as well as to identify the key elements within both disciplines, the two articles will be studied separately. Afterward, the attention will shift to the recently introduced GDPR, in order to find out whether the protection of the elements, introduced by this directive, are applicable to Bitcoin technology or not.

2.1.1 Right to privacy within the ECHR framework

The ECHR mentions right to privacy within article 8, despite its nomenclature says "Right to respect for private and family life". The text of the article read as follow:

"*1. Everyone has the right to respect for his private life and family life, his home and his correspondence.*

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".[99]

Article 8 contains a particular guarantee for what concerns the protection of privacy. Four different spheres of protection are named within the text: private life, family life, a person's home and correspondence. Despite their different nomenclatures, these four spheres cannot be clearly distinguished from one another. On the contrary, it was said that they may rather overlap in various

98 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML, accessed the 30th may 2018

99 European Convention on Human Rights, art.8

aspects, forming a broad guarantee for an individual's freedom, indispensable for a person's personality development.[100] The essential purpose of this article is to protect the individual against arbitrary interferences by the public authorities with his private (and family) life, in order to secure to the individual a sphere within which he/she can freely pursue the development of his/her personality. Both in literature and in the legal discourse, privacy has been regarded as a subjective right of the individual to protect his/her personal interests, such as relating to human dignity, individual autonomy and personal freedom.

2.1.2 Right to Privacy in the EU Charter of Fundamental Rights

When it comes to right to privacy within the legal framework of the EU Charter of Fundamental Rights, a legal analysis can't just consider the solely provision of Article 7, since its corresponds to Article 8(1) of the ECHR, and it focuses primarily on individual autonomy. More specifically, article 7 says that:

"*Everyone has the right to respect for his or her private and family life, home and communications.*"[101]

Despite there was the willingness of taking into account new technologies and the contemporary technological development, by replacing the word "correspondence" with "communications", the scope of this article follows slavishly that of article 8 of ECHR.
It becomes therefore necessary, in the legal analysis of the EU Charter framework, to go further and take into exam what is established by Article 8 regarding the issue of data protection. The text of Article 8 of the EU Charter reads as follow:

"1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."[102]

The right to respect for private life and the right to personal data protection, although seem closely related, are distinct rights. Indeed, they both strive to protect similar values, such as the autonomy and human dignity of individuals, by granting them a personal sphere in which they can freely

100 D.J.Harris, M. O'Boyle, E. Bates et al., "*Harris, O'Boyle & Warbrick, 'Law of the European Convention on Human Rights",* Oxford Univ. Press, ed. 2014, p. 245-261.

101 EU Charter of Fundamental Rights, article 7.

102 EU Charter of Fundamental Rights, article 8

develop their personalities, think and shape their opinions. They are thus an essential prerequisite for the exercise of other fundamental freedoms, such as freedom of expression, freedom of peaceful assembly and association, and freedom of religion. Nevertheless, the two rights differ in their formulation and scope. The right to respect for private life consists, as we have seen previously, in a general prohibition of States and third parties' interferences, subject to some public interest criteria that can justify interference in certain cases.

New information and communication technologies have led to the automatic processing of personal data from both the public and private spheres without regard to frontiers.[103] This has contributed in creating new and unprecedented risks of infringement of respect for private life. Therefore, the compilers of the Charter devoted a specific article to the protection of personal data, in order to give it an appropriate treatment.[104] Article 8 of the Charter recognizes hence the right to the protection of personal data as a new fundamental right, distinct from the right set out by Article 7. The protection of personal data is viewed as a modern and active right, putting in place a new system of checks and balances to protect individuals of which personal data are processed.[105] The processing must comply with the essential components of personal data protection, namely independent supervision and the respect for the data subject's rights. The right to personal data protection comes into play whenever personal data are processed; it is thus broader than the right to respect for private life. Any processing operation of personal data is subject to appropriate protection. Data protection concerns all kinds of personal data and data processing, irrespective of the relationship and impact on privacy. Processing of personal data may also infringe on the right to private life, as shown in the examples.

2.1.3 The right to Privacy in the EU regulations on ePrivacy and General Data Protection.

Close to the two aforementioned human rights treaties, within the EU there are two important directives which have shaped the regulatory environment for privacy and data protection: the ePrivacy regulation (ePR) and the recently entered into force General Data Protection Regulation (GDPR). Although these regulations are not specifically human rights instruments, they must be

103 EU network of independent experts on fundamental, COMMENTARY OF THE CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, June 2006, p.90, available at http://www.pedz.uni-mannheim.de/daten/edz-k/gdj/06/network_commentary_final%20_180706.pdf, (accessed the 7th June 2018)

104 Ibidem

105 On this point, Advocate General Sharpston described the case as involving two separate rights: the "classic" right to the protection of privacy and a more "modern" right, the right to data protection. See CJEU, Joined cases C-92/09 and C-93/02, *Volker und Markus Schecke GbR v. Land Hessen*, Opinion of Advocate General Sharpston, 17 June 2010, para. 71, available at http://curia.europa.eu/juris/celex.jsf?celex=62009CJ0092&lang1=en&type=NOT&ancre, accessed the 7th June 2018

interpreted in the light of the provisions on privacy and data protection given by EU Charter and the ECHR.

The development of new technologies, more specifically of social media platforms, has remarkably contributed to the surge of personal data shared on the Internet by its users through social networking, community building and user-generated content production.[106] This huge quantity of data, together with lower storage costs and more sophisticated data mining techniques, have increased profiling abilities of governments and commercial actors. The systematic monitoring of individuals has given rise to the phenomenon commonly known as *dataveillance*.[107] More specifically, online platforms are based on a data-driven model in which personal data constitute an economic asset, the "new oil" or "new currency" of the digital world.[108] Personal data has become the new form of payment used in the digital market in order to obtain access to online services. Moreover, in these online contexts, users often have a low control over their data that goes along with a lack of sufficient knowledge able to give a free and informed consent. This may pose serious risks for privacy as data controllers can draw invasive inference about the users, contributing in creating a so-called "*black-box society*".[109] In this kind of society individuals don't have a meaningful control over their data. This exacerbates the risks of stigmatization, reinforcement of stereotypes, discrimination, social and cultural exclusion is of high concern. The European commission has identified numerous areas of concern on this point such as "minimization, purpose limitation, data retention/deletion, automated decision taking/profiling and security requirements".[110] In order to cope with the challenges of the black-box society, on 14th April 2016 the EU Commission, Parliament and Council of Ministers agreed on the General Data Protection Regulation (GDPR). This Regulation has two main aims: reinforce data protection of personal data across European member states by giving more control to individuals over their data, on one hand; facilitate the free flow of personal data in the Digital Single Market, on the other hand.[111]

106 R. Filippone, "Blockchain and individuals' control over personal data in European data protection law", Master Thesis, Tilburg University, August 2017, p.5 available at http://arno.uvt.nl/show.cgi?fid=143638 (accessed the 10 June 2018),

107 R. Clarke, 'Dataveillance by Governments', in *Information Technology & People*, Vol.7, iss. (2), 01 June 1994, pp.46-85

108 R. Filippone, "Blockchain and individuals' control over personal data in European data protection law", Master Thesis, Tilburg University, August 2017, p.5 available at http://arno.uvt.nl/show.cgi?fid=143638 (accessed the 10 June 2018),

109 F. Pasquale, "The black box society: the secret algorithms that control money and information", 2015, Cambridge: Harvard University Press. from https://www-degruyter-com.uaccess.univie.ac.at/view/product/430038 (accessed the 11 June 2018)

110 EU Commission, "Report on Public Consultation on the IoT Governance', 2013, available at https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation, (accessed the 11 June 2018)

111 R. Filippone, "Blockchain and individuals' control over personal data in European data protection law", Master Thesis, Tilburg University, August 2017, p.6 available at http://arno.uvt.nl/show.cgi?fid=143638 (accessed the 10 June 2018).

GDPR aims to increase data controllers' tasks and duties, by fostering the pivotal role of individuals in exercising a major control over their data. In doing this, the new EU regulation has strengthened some of already existing individuals' rights and it has introduced new ones, such as the 'right to data portability' and the 'right to be forgotten'. Moreover, new forms of protection of data, such as the 'pseudonymisation' were disciplined for the first time. The new legal framework seeks hence to alter the relationship between data controllers and data subjects, in the direction of a more balanced relationship between businesses and individuals when it comes to the sharing of the benefits of big data.[112] The processing of customers' personal data – often realized without customers' consensus – leads to significant profits for those organizations who built their businesses on these activities. Bearing in mind these contexts, the GDPR aims to put individuals in the condition of increase the knowledge of how their data are used and how to use them for their purposes.[113] The achievement of this aim is stressed since the opening clauses of the Regulation. Recital (7) of GDPR in fact affirms that "*Natural persons should have control of their own personal data*"[114] The idea of empowering individuals' control over their data was already stressed by the European Commission back in 2012, when it was said that the aim of a European Data Protection framework should have been to "*give people efficient and operational means to make sure they are fully informed about what happen to their personal data and to enable them to exercise their rights more effectively".*[115] The strengthening of individuals' control was realized in two ways. On one hand, by introducing a series of measures aiming to equip individuals of some 'micro-rights' relating to different stages of data processing, such as the right to access, right to data portability and the right to be forgotten. On the other hand, by creating a new series of elements which encompasses technical and organizational measures able to:

- enforce security measures;

- increase the responsibility and accountability of data controllers;

- introduce the principles of privacy-by design and by default;

112 Ibid., p. 7

113 Ibid.

114 (EU) REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), GDPR, Recital 7, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, (accessed 12 June 2018)

115 P. Silva, "*A European Data Protection Framework for the 21st century. Safeguarding Privacy in a Connected World*", available at https://hrmi.lt/wp-content/uploads/2016/11/Paolo-Silva_Presentation-Digital-Rights-Forum.pdf, accessed the 12 June 2018

- enhance administrative and judicial remedies.[116]

The ultimate aim of these measures is to create an environment which aims to enhance the concept of privacy, through the adoption of specific technical and organizational elements. This could be achieved in a twofold manner: shaping the data processing architecture, in the respect of the fundamental rights and interests of the individuals, on one hand; imposing a higher level of transparency in order to strengthen its control, on the other hand. In order to empower the individuals' control over the treatment of their data, new principles, rights and requirements have been introduced for the first time within the GDPR.

Pseudonymisation (Article 4(5) GDPR)[117]*:* GDPR defines pseudonymisation as*: 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.* With the introduction of "pseudonymisation" within the new legal framework, the GDPR acknowledges the high importance of pseudonymisation in order to grant effective data protection. The Regulation mentions not only pseudonymisation within the recitals, but also provides a definition and several Articles concerning pseudonymisation as a very useful data security measure.

The word 'pseudonymisation' in the GDPR thus refers to a process which reduces the risk of direct identification, but which does not produce anonymous data. Thanks to pseudonymisation is used as a mean to reduce risks to data subjects, as well as an appropriate safeguard for any personal data used for scientific, historical or statistical research.[118] Pseudonymisation requires also a very specific form of data protection. According to the definition afore given, while the pseudonymisation process requires *'technical and organisational measures*', it is indeed the '*additional information*' which must be '*subject*' to these measures.[119] The core of the protection it must be given to the additional identifiable information, which are held separately from the pseudonymised data. Therefore, the 'only' risk of identification mitigated against within GDPR pseudonymisation is

116 R. Filippone, "Blockchain and individuals' control over personal data in European data protection law", Master Thesis, Tilburg University, August 2017, p.22-24 available at http://arno.uvt.nl/show.cgi?fid=143638 (accessed the 10 June 2018),

117 (EU) REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), GDPR, Article 4., available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, (accessed 12 June 2018)

118 M. Moruby, E. Mackey, M. Elliot & Others, "Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK", in *Computer Law & Security Review*, April 2018, Vol. 34, iss.2, pp.222-233.

119 Ibidem.

the risk of identification through the original data held by the controller.[120] In this regard, Recital 29 of GDPR give further clarifications about these pseudonymised data: "*In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should (…) be possible within the same controller, when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately*".[121] From a joint reading of article 4 (5) and recital [29] it follows that the control needed for the protection of pseudonymised data is the one who takes care of the 'internal' risk of identification from additional information retained by the data controller. This identification risk is not only limited to the danger posed by the original identifying data, but also to any means which could be used by the identification of these identified data.

Right to be forgotten. (Article 17 GDPR).[122] According to this right, natural persons should have granted "*(…) the right to obtain from the controller the erasure of personal data concerning him or her without undue delay (….)*". Although this right has been formally introduced with the GDPR, already in the DPD has been set forth the principle according to which personal data should be kept only as long as they are necessary for the purpose of collection.[123] Moreover, in 2014 the same Court of Justice of the European Union recognized, in the "*Google Spain v. AEPD and Mario Costeja Gonzalez"* case, the existence of the right to be forgotten. In this landmark decision, the ECJ has declared that individuals have a so-called 'right to be forgotten', that is, the right to demand search engines to erase search results obtained through searches for their names. The Court

120 Ibidem

121 (EU) REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), GDPR Recital 29.

122 (EU) REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), GDPR Article 17 says: 1. *The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). 2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. 3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims.*

123 R. Filippone, "Blockchain and individuals' control over personal data in European data protection law", Master Thesis, Tilburg University, August 2017, p.25 available at http://arno.uvt.nl/show.cgi?fid=143638 (accessed the 10 June 2018),

recognized the obligation of search engine operators in removing links to webpages showed among the results of a query when they are "*inadequate, irrelevant, or no longer relevant, or excessive in relation to the purposes of the processing at issue".*[124] The ECJ has however specified that this is not an absolute right, but it has to be demonstrated by the applicant the lack of a "preponderant interest" in having access to the information.[125] The right of be forgotten is the expression of the fundamental right to have control over certain aspects of one's life, such as making choices and taking informed decisions.[126] The control over personal data allows to show different aspect of the inner self to chosen people according to determined context. This right to informational self-determination has been recognized and protected as a right to the protection of personal data which allows individuals to full self-determine their lives, without being periodically associated with past actions.

Data protection officer (Article 37 GDPR).[127] Among the new introductions provided by the new EU GDPR it has to be recalled the new figure of Data Protection Officer (DPO). The idea of adopting a professional figure of this kind was already circulating in the European Union framework since the beginning of 2012. Within an official communication of that period, it was proposed to introduce a professional figure able to enhance the accountability of processing data breaches.[128] Nowadays, Article 37 of GDPR requires to organisations to appoint a data protection officer when these three specific conditions appear:

---

124 ECJ, *Google Spain v. AEPD and Mario Costeja Gonzalez*, 13th May 2014, §94 available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=IT

125 Ibid., §100

126 C.de Terwangne, "The Right to be Forgotten and the Informational Autonomy in the Digital Environment", European Commission Joint Research Centre Institute for the Protection and Security of the Citizen, Luxembourg , 2013, p. 6, available at http://publications.jrc.ec.europa.eu/repository/bitstream/JRC86750/jrc86750_cecile_fv.pdf, (accessed the 13 June 2018)

127 (EU) REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), GDPR Article 37 says: "*1. The controller and the processor shall designate a data protection officer in any case where: a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; c). or the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10." 2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment. 3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size. 4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. 2The data protection officer may act for such associations and other bodies representing controllers or processors. 5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39. 6. The data protection officer may be a staff member of the controller or processor or fulfil the tasks on the basis of a service contract. 7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority."*

128 "Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century", 25.1.2012, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en, (accessed the 14 June 2018). The part of the text in which is required the creation of this figure states: "*by requiring data controllers to designate a Data Protection Officer in companies with more than 250 employees and in firms which are involved in processing operations which, by virtue of their nature, their scope or their purposes, present specific risks to the rights and freedoms of individuals (risky processing".*

1. If the data is processed by a public authority or body, except for courts acting in their judicial capacity;
2. If the controller's or processor's core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale;
3. If the controller's or processor's activities consist of processing large quantities of special categories of data and personal data relating to criminal convictions and offences.[129]

In practice, these conditions will cover a large number of organisations, and it wouldn't be unusual to see companies appoint a DPO even if they're not strictly required to.[130] DPO has hence the role of circumscribing the risks of a widespread diffusion of special categories of data. The latter are expressly mentioned in Article 9 of the Regulation; more specifically, these data are those which "*reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or (..) data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited*".[131] The DPO's duties generally revolve around ensuring that the data controller and data processor comply with all relevant data protection legislation, especially the GDPR. They should also offer advice, monitor data protection impact assessments and operate as the immediate contact for the supervisory authority. The appointment of a professional figure such as the DPO it has to traced back to the aforementioned intention of the new Regulation of empowering individuals' control through enhancing the accountability of data controllers.

2.2. The Right to Property

2.2.1. The problem of a univocal definition within the European Union.

Next to the right to privacy, another right that is affected by the long-standing lack of an *ad hoc* regulation of the Bitcoin phenomenon is undoubtedly the right to property. Despite this right finds its legal discipline within both the ECHR and the EU Charter of Fundamental Rights, many difficulties arise when it comes to giving a definition of this right. Within the European context, the protection of the right of property has traditionally taken place only at the national level, while its supranational safeguard has until relatively recently been hindered due to two main reasons. The

129 (EU) REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), GDPR Article 37 says

130 A. Calder, *"EU GDPR A Pocket Guide"*, United Kingdom, IT Governance Publishing, 2016, p. 51

131 EU REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), GDPR, article 9

close relationship of the idea of property as a fundamental right with each State's political and ideological orientations, on the one hand, and the perception of property as an institution closely related to the national political, economic and social policies, on the other, have rendered it difficult for decades to build an integrated system of protection for the right of property at the European level.

The word 'property', as used by lawyers, is a dangerously slippery word, in open contradiction with a profession, the legal one, which boasts of its precision.[132] Peter Birks, in his script "Before we begin: five keys to land law", has distinguished between the use of the label 'property' to loosely mean 'the wealth of an individual', and a stricter, more technical, usage of the word.[133] In this more technical usage, according to Birks, property is clearly distinguishable from its related obligations by one 'simple' question: "Against whom is this right exigible?". This question has then generated the dichotomy whether right to property can be meant or as a right *in rem* or right *in personam*. A right *in rem* is a right which exigibility is defined by the location of a thing, while a right *in personam* is defined by the location of the person.[134] This narrow definition creates even more problems when it comes to qualify the so-called 'bank money'[135] as a property. In this particular context, in fact, 'property' is meant as something different from the classical *in rem* right, due its undeniable nature of right *in personam*. Next to the distinction operated by Birks, there is an even more plain definition of property, according to which one of the hallmarks of a property right is its exigibility against strangers to its creation.[136]. According to this view, debts, including then also those constituted on incorporeal money, could not be qualified as property at all. Such a narrow definition of property better enables to make clear that *in personam* 'not-property' works totally differently from *in rem* properties. It is indeed preferable a broader definition of property, since it is able to encompasses all those similarities in legal rules applicable to both transferable *in rem* and transferable *in personam* rights. The legal rules applicable to all transferable rights, represented by the general rule *nemo dat quod non habet,* are in open countertendency with the narrow conception provided by Birks. A broader definition of property is hence able to refers to the law recognition of and willingness to enforce a holder's right to exclude others from the enjoyment of a particular good.

132 K.F.K. Low & G.S.Teo, "Bitcoins and other cryptocurrencies as property?", in *Law, Innovation and Technology,* vol. 9, no. 2, 2017, pp, 235-268. .

133 P. Birks, "Before we begin: five keys to land law", in S. Bright and J. Dewar ed., *Land Law: Themes and Perspectives,* Oxford, Oxford University Press, 1998, pp. 457-486, p. 473

134 K.F.K. Low & G.S.Teo, "Bitcoins and other cryptocurrencies as property?", in *Law, Innovation and Technology,* vol. 9, no. 2, 2017, p. 242

135 J.M. Keynes, *A Treatise on Money*, Harocurt, Brace, 1930, vol.1, pp. 5-6

136 W. Swadling, 'Property: General Principles', in A. Burrows (eds). *English Private Law,* Oxford, Oxford University Press, 2103, pp. 173-306

The right of property, like other rights, is protected in Europe through the overlapping of three distinct legal frameworks: the national framework, the EU framework -with the ECHR- and the Council of Europe. Each of these laws has its own scope of application and level of protection, which partially differ from those of the others, as well as its own supreme jurisdiction which seeks for itself the final decision in the field of human rights law.[137] The role of law became therefore crucial in order to identify the person holding this 'right to exclude'. Under this point of view, legal developments materialized in Europe during the last sixty years have markedly changed this scenario. Hence, nowadays, the safeguard of the right to property is no longer reduced to the national field, but it rather takes place at the interface between international law, EU law and each national legal discipline.[138]

As it was done in the first part of this chapter, the main purpose of this chapter will be, after providing a legal analysis of the different European sources disciplining the protection of the right to property, to see whether the current legal frameworks are applicable also to the bitcoins' ownership and to understand if bitcoins' owners are sufficiently protected against risks of property deprivation.

2.2.2. The 'Protection of Property' within the ECHR framework.

Within the legal order adopted under the auspices of the Council of Europe, the right of property was not included in the first draft of the ECHR, signed in 1950 in Rome, but in the First Protocol to the Convention promulgated two years later, in 1952. This situation was the result of the divergences among the States present at the Council of Europe regarding the very idea of property and involves a compromise by virtue of which certain flexibility is conferred to the States, which can opt for ratifying the Convention but not the Protocol.[139] The formulation adopted in the first Protocol provides a qualified definition of the right to property, by allowing States a wide power to interfere with that right.[140] Article 1 of the First Protocol reads as follow:

"1. Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.

137 D.U. Fernandez-Bermejo, "The multilevel protection of the right of property in Europe", in *China-EU Law Journal*, vol.4, 2015, pp.75-103

138 Ibidem, p. 76

139 Up to now, 4 july 2018, the only States that have not ratified this protocol are Monaco and Switzerland. See https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/009/signatures?p_auth=niytbJxY, accessed the 4th July 2018.

140 A. Grgic, Z. Mataga & Others, "*The right to property under the European Convention on Human Rights, A guide to the implementation of the European Convention on Human Rights and its protocols*", Belgium, June 2007, p. 5, available at https://rm.coe.int/168007ff55 (accessed the 16 June 2018)

2. The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties"[141]

Article 1 introduced three distinct but interrelated rules: a) the general principle of peaceful enjoyment of property; b) the protection against any deprivation of possessions and c) the guarantee concerning the control of the use of property. From a first reading, the interrelationship between these three principles is evident. The second and the third rule constitute special cases of interferences of the right to property, which should be interpreted in the light of the first principle. When a trial comes to the ECtHR, this interrelation becomes decisive for the admission of the case. Before considering whether the first rule was complied with, the Court will firstly examine if the other two rules were applicable or not.

The concept of 'possessions', in the authentic language versions of the Protocol, used to express a broad international legal concept of property. According to the Court, the notion 'possessions' has an autonomous meaning that is not limited to the ownership of physical goods and which is independent from the formal classification in domestic (national) law, being thus possible to regard certain other rights and 'legitimate expectations' constituting assets as 'property rights', and thus as 'possessions', for the purposes of the alluded provision.[142] In order to determine whether such 'legitimate expectations' exist, the ECtHR has indicated that it is not its task to decide whether or not a right of property exists,[143] but the claim must find sufficient legal basis under the domestic law of the respondent State. Article 1 of Protocol No. 1 does not guarantee the right to acquire property. Nevertheless, this does not mean that the notion of "possessions" is limited to "existing possessions".[144] Other assets, including claims in respect of which an applicant can argue that he or she has at least a "legitimate expectation" that they will be realised, qualify as "possessions". It is important to stress that a mere hope of securing an asset is *per se* not sufficient to establish a property within the meaning of Article 1. A claim may be regarded as an asset only when it is sufficiently established to be enforceable. The conspicuous jurisprudence of the ECtHR has affirmed that the term 'property' includes not only physical goods, chattels and immovable objects,

141 ECHR, Optional Protocol 1, adopted the 2o March 1952

142 See, among others, ECtHR, *Gasus Dosier-und Fördertechnik GmbH v. The Netherlands*,no. 15375/89. 21 December 1992, para. 53; ECtHR, *Beyeler v. Italy*, no. 33202/96, 5 January 2000, § 100.

143 ECtHR, *0 Matos e Silva, Lda. and Others v. Portugal*, no. 15777/89, 16 September 1996, §. 75.

144 A. Grgic, Z. Mataga & Others, "*The right to property under the European Convention on Human Rights, A guide to the implementation of the European Convention on Human Rights and its protocols*", Belgium, June 2007, p. 7, available at https://rm.coe.int/168007ff55 (accessed the 16 June 2018)

but also more 'abstract' concept as intellectual property,[145] economic interests -such as claims on taxes or other contributions,[146] welfare benefits[147] and eventually inheritance rights.[148.]

2.2.3- The Right to Property within the EU Charter of Fundamental Rights

Since 2009 the right to property has been recognized as a fundamental constitutional right in all Member States of the EU and it is therefore protected both as a general principle of EU law and as a fundamental right expressly contained in Article 17 of the EU Charter of Fundamental Rights. Under the heading ''right to property'', this provision, establishes:

"*1. Everyone has the right to own, use, dispose of and bequeath his or her lawfully acquired possessions. No one may be deprived of his or her possessions, except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for their loss. The use of property may be regulated by law in so far as is necessary for the general interest.*

2. Intellectual property shall be protected."[149]

Even though Article 17 CFR is more detailed (referring expressly to the protection of intellectual property, to the duty to pay fair and prompt compensation in case of deprivation of property, or to the essential aspects defining the powers of the owner), its content and structure are clearly similar to those Article 1 of the Protocol 1. Such similarity is not unintentional. According to the explanations relating to the Charter, which are to be followed by the Courts of the EU and by the member States when interpreting the Charter, Article 17 CFR is based Article 1 of the Protocol 1.[150]

2.3 The Right to Work

The value of the work is assuming a growing importance in today's world. Work is instrumentally valuable, as productive labour generates: goods needed for survival, good needed for self-development as well as other material goods that people wish to have in order to live a fulfilling life. Work is not only valuable for the income it generates, but it is also crucial for a person's feeling

145 See among the others, ECtHR, *Balan v. MDA*, No. 19247/03, 29 January 2008, par.34 et seq; ECtHR, *Anheuser-Busch Inc. v. Portugal*, n. 73409/01, 11 January 2007, par. 72; ECtHR, *Paeffgen GmbH v. Germany*, No. 25379/04, 18 September 2007.

146 ECtHR, *Darby v. Sweden*, No. 11581/85, 23 October 1990, par.30; ECtHR, *Dangeville v. France*, 36677/97, 16 April 2002, par. 48.

147 ECtHR, *F.Lombardo v. Italy*, No. 11519/85 & No. 12490/86, 26 november 992, par. 16 & par. 17.

148 See. 112; ECtHR, *Négrépontis-Giannis v. Greece*, No. 56759/08, 3rd May 2011, par. 97, 104.

149 EU Charter of Fundamental Rights, Article 17.

150 'Explanations relating to the Charter of Fundamental Rights'(14/12/2007), OJ C 303, p7, when it comes to Article 17 it is immediately stated that "*This Article is based on Article 1 of the Protocol to the ECHR'*., see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007X1214(01)&from=EN, accessed the 6 July 2018.

of membership in society. Moreover, through his/her work, an individual gives a further contribution within the society, by paying taxes on the incomes, allowing the central governments of allocate these taxes in the implementation of public utilities and services. In order to evaluate whether it is possible to consider the right to work as a human right, three possible approaches have been formulated.[151] A first approach is a positivistic approach, according to which the right to work is a human right if it is explicitly mentioned in human rights document. A second approach is an instrumental one; according to this approach, the right to work is configurable as a human right if courts protect is as such or if civil society organisation succeed in using it strategically aiming to promote relevant goals. A third approach finds its justification within the normative sphere of application. Right to work is a human right if there are certain human interests of sufficient importance to impose duties on others.

2.3.1 The right to work in the ECHR

Despite the fact that the ECHR doesn't explicitly recognise the right to work, it contains a number of rights which can be traced back to the labour sphere. Namely, these rights are: the prohibition of slavery, servitude, forced and compulsory labour, [152] the freedom of association,[153] including the right to form and join trade associations and, eventually, the prohibition of discrimination,[154] which is not a free-standing right, but it can be only violate in conjunction with other Convention provisions. The protection of the right to work is enhanced, both in case law as in literature, also with regard to the place of work should be included also protection. Several factors are considered in this sense: from the unfair dismissal for activities outside work,[155] to the health and safety conditions at work,[156] collective labour rights, religion and dismissal and eventually the protection against slavery and servitude.

Even though the ECtHR doesn't protect the right of everyone against the state to obtain a job in order to make a sustainable living, nevertheless it has recognized a bunch of principles which

151 V. Mantouvalou, The Protection of the Right to Works Through the ECHR, in *Cambridge Yearbook of European Legal Studies*, vol. *16*, 2012, pp. 313-332.

152 ECHR, Art. 4: 1. No one shall be held in slavery or servitude. 2. No one shall be required to perform forced or compulsory labour. 3. For the purpose of this Article the term "forced or compulsory labour" shall not include: (a) any work required to be done in the ordinary course of detention imposed according to the provisions of Article5 of this Convention or during conditional release from such detention; (b) any service of a military character or, in case of conscientious objectors in countries where they are recognised, service exacted instead of compulsory military service; (c) any service exacted in case of an emergency or calamity threatening the life or well-being of the community; (d) any work or service which forms part of normal civic obligations.

153 ECHR, Art. 11: 1. Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.

154 ECHR, Art, 14: The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

155 H. Collins and V. Mantouvalou, *'Redfearn* v. *UK:* Political Association and Dismissal', in *Moder Law Review*, vol. 73, 2013, p.909.

156 ECtHR, *Vilnes and o. v. Norway*, No. 52806/09 and 22703/10, 5 December 2013.

underpin the importance of the work in an individual's daily life. These principles can be summed in four different categories:

1) Livelihood for dignity: the ECtHR has affirmed that livelihood gained through work is essential for human dignity, by adding value to the instrumental conception of work as a means of incomes.[157] In this sense, the Convention doesn't protect salaries as such, with a provision on a right to a minimum wage. Instead, the Court has classified salaries as 'possession',[158] allowing in this way to make them fall under the provisions of Article 1 of Protocol 1.

2) Prohibition of exploitation: decent working conditions are an essential part of the right to work. In perpetrating exploitative practices, it is perpetrated an abuse of the vulnerability of a worker, through the violation of labour standards and other human rights, in order to obtain profits. Moreover, these forms of labour exploitation contribute in creating the so-called 'precariousness', which makes workers prone to be exploited.

3) Self-realisation: The Court has emphasized the function of the work as a form of self-realisation in one person's life. In this sense, the workplace plays an essential role, since is the place where people flourish by developing social relationships. The fact that the Court has recognized the value of self-realization through work doesn't imply that individual applicants who don't have sufficient opportunities of self-realisation can bring a successful complaint to Strasbourg.

4) Non-domination: according to this principle, and in order to see the effective protection of the right to work, as well as to achieve a self-realisation, a worker has to be protected from domination in the workplace. Concretely speaking, the power of dominate exists when someone has the capacity to interfere with another person's choices on an arbitrary basis. Despite the inherent subordinate nature of the employment relationship, which creates de facto an imbalance of powers, the Court has affirmed on a person's dismissal has to be operated fairly and regardless of factors not related to the working environment.[159]

157 ECtHR, *Young, James and Webster v UK*, No. 7601/76 and 7806/77, 13 August 1981, §.55;

158 ECtHR, *Evaldsonn and O.v. Sweden*, No. 75252/01, 13 February 2007

159 ECtHR, *Redfearn v. UK*, No. 47335/06, 6 Novmber 2012, §§ 43-48

2.3.2 The right to Work in the EU Charter of Fundamental Rights

Contrary to what it has been said about the ECHR, where the protection of the right to work comes from the combination of other articles of the convention, in the EU Charter we have an explicit provision. Article 15 introduces the discipline of the 'freedom to choose an occupation and the right to engage in work'. The text says:

1. *Everyone has the right to engage in work and to pursue a freely chosen or accepted occupation.*
2. *Every citizen of the Union has the freedom to seek employment, to work, to exercise the right of establishment and to provide services in any Member State.*
3. *Nationals of third countries who are authorised to work in the territories of the Member States are entitled to working conditions equivalent to those of citizens of the Union.*[160]

This article has to be integrated with three other dispositions of the EU Charter: Article 30, who provides the protection against unfair dismissal;[161] Article 31, which guarantees fair working conditions;[162] and article 32, which prohibits child labour and protects young people at work.[163.]

In addition to the principles already stated in the ECHR, the EU Charter goes further, by providing, in Article 15 (2), the freedom to move, settle and provide services. Article 15(2) gives EU citizens enforceable rights before any national court. "This could have implications for the justiciability of Article 15 as a whole, including Article 15(1), despite given its more ideological and political dimension."[164]

PART II
– THE STATES OBLIGATIONS IN RELATION TO HUMAN RIGHTS DISCUSSED –

160 EU Charter of Fundamental Rights, Article 15.

161 EU Charter of Fundamental Rights, Article 30: "Every worker has the right to protection against unjustified dismissal, in accordance with Union law and national laws and practices"

162 EU Charter of Fundamental Rights, Article 31: "1. Every worker has the right to working conditions which respect his or her health, safety and dignity. 2. Every worker has the right to limitation of maximum working hours, to daily and weekly rest periods and to an annual period of paid leave."

163 EU Charter of Fundamental Rights, Article 32:" The employment of children is prohibited. The minimum age of admission to employment may not be lower than the minimum school-leaving age, without prejudice to such rules as may be more favourable to young people and except for limited derogations. Young people admitted to work must have appropriate working conditions to their age and be protected against economic exploitation and any work likely to harm their safety, health or physical, mental, moral or social development or to interfere with their education."

164 B.Bercusson, *'European labour law and the EU Charter of Fundamental Rights'*, Brussels, ETUI, Brussels, 2002, p.31.

2.4 The State obligations concerning the Right to Privacy.

2.4.1 State obligations according to ECHR

Article 8 of ECHR imposes positive and negative obligations on States. Regarding positive obligations Grabenwarter, in its commentary on ECHR, has affirmed [165] that there are kinds of obligations:

- obligations to protect the individual from third parties' interferences;
- obligations applicable with regard to organisation and procedures:
- obligations to inform.

In referring to the first obligation, States are obliged to safeguard the private sphere of an individual by all those potential risks for his/her privacy. More specifically, these risks may harm, for instance, the right of sexual self-determination of an individual, or his/her moral integrity, or his/her reputation or the right to one's own picture and eventually the illicit diffusion of his/her personal data. States have to comply with these positive obligations, by guaranteeing an effective respect for private life through its legislative, executive and judicial authorities. These authorities, then, must ensure the actuation of appropriate protection to the individuals affected by violations of their privacy.

As second, positive obligation, Article 8 imposes therefore organisational and procedural duties on the Member States. Since article 8 doesn't contain any explicit procedural requirements, the decision-making process leading to measures of interference must be fair and such as to afford due respect to the interests safeguarded by the same Article 8.[166] As third positive obligations, Article 8 imposes the duty to inform. This obligation has to be accomplished whenever some data are collected in order to pursue a legitimate aim and to contribute to the effectiveness of national proceedings, as well as protect the interests of the person concerned. Despite the ECHR disciplines the right to receive information at article 10, there are cases in which the two provisions are intertwined and the more the data on a subject are sensitive and helpful, the faster this data has to be shared with the person concerned.

As for the negative obligations, the respect of an individual's privacy does not merely compel the central authority to abstain from perpetrating any unlawful investigation or interference into one's

165 C.Grabewarter, *ECHR: a commentary*, C. H. Beck (eds), Bloomsbury Publishing PLC, 2014, p.219

166 ECtHR, *Taşkın and Others v Turkey*, No. 46117/99, 30 March 2005, §118

privacy, but it obliges also the same State to protect individuals' privacy by any intromission by third parties. The State has the duty of non-interfering within the private aspects of its citizen, refraining by introducing also all those invasive measures which may contribute in these interferences. When it comes to possible state interferences to private life of an individual, the threshold between violation or non-violation could be very blurred. There are specific situations in which the State is justified in interfering within an individual's private life, and therefore to collect sensitive or personal data. This happens when the interference is prescribed by law, and therefore justified by its intrinsic legitimate aim. To determine whether an infringement of the right to privacy was prescribed by law, the question which needs to be asked is whether there was a legal basis granting a power to the governmental organization involved and whether the conditions for using that power were respected. On this point, Article 8 (2) lists a wide range of these possible legitimate aims for the justification of an interference such as for reasons of national security and public safety, the prevention of disorder or crime, the protection of health or morals and of the rights and freedoms of others.

The national law must be clear, must be made public and must be foreseeable as to its consequences. [167] Furthermore, the interferences of the State must be proportional, which means that a fair balance has to be struck "between the general interest of the community and the interests of the individual each time".[168] It constitutes a lawful restriction of article 8 when certain tools are used for the acquisition or information such as, for instance, during police investigations. Due to the possibilities of modern computer-based collection and analysis of data, the protection of personal information within the technological framework became an important part of the guarantees under article 8. According to European Court of Human Rights' interpretation, the beneficiaries of Article 8 provisions are all the natural persons or groups of individuals.[169] Article 8 has been interpreted by the Court in such a way that it primarily aims at protecting individual interests by granting natural persons the right to complaint in order to see the protection of their rights. These individual interests, which embrace those spheres of the individual personality such as autonomy, dignity and personal development, constitute therefore the minimum threshold for the acceptance of a proceeding before the court. Cases that do not regard such private matters are, in principle,

167 D. Melkonyan, '*Concept of the rule of law in the case-law of the European Court of Human Rights*', available at http://ysu.am/files/Davit_Melkonyan-1415702096-.pdf, accessed the 1st June 2018.

168 ECtHR, *Rees vs. UK*, 9532/81, 17 October 1986, § 37

169 On this point, a clarification has to be made. When it comes to groups, the Court has stated that are entitled to submit a complaint to the competence of the Court only groups of different individuals which have been affected by the same breach of their right to privacy. It is not allowed to bundle complaints on behalf of a groups or as a group, such as Gypsies, Muslims or Catalans.

rejected by the Court. On this point, furthermore, the ECtHR has stressed that an application will only be declared admissible if it concerns a concrete and direct interference with the right to privacy of the applicant, who has hence the burden of proving that this concrete interference took place.

Linked to the legal-basis criterion, the European Court of Human Rights has introduced another sub- requirement, named *'the quality of law*'.[170] With particular reference to the mass surveillance cases, for instance, the Court has given a particular emphasis on the safeguards against any possible arbitrary use of power when it comes the implementation of those measures of secret surveillance. The Court went on, saying that: "*the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, giving then to the individual the adequate protection against arbitrary measures.*"[171] By doing this, ECtHR has increasingly adopted the role of a 'European constitutional court',[172] rather than its classic role of human rights court.

2.4.2 State obligations according to EU Charter

Even for what concerns the right to data protection, in quality of fundamental right, the protection of personal data does not merely require that the Member States bodies abstain from illegal interferences in the personal data. It also exists a positive obligation to secure the protection of personal data. As it was stressed during the analysis of Article 8 ECHR, States' positive obligations presuppose the adoption of legislation laying down more precise rules and principles concerning the protection of personal data. In accordance with the provisions of Article 8, paragraph 2, of the Charter the protection of personal data shall be exercised in compliance with the conditions and limits defined by the measures adopted to give effect to it. [173]

The structure and wording of the EU Charter is also different than that of the ECHR when it comes to lawful interferences. The Charter does not use the notion of interferences with guaranteed rights but contains instead a specific provision on limitation(s) on the exercise of the rights and freedoms recognised by the Charter.[174] On this point, in fact, Article 52 (1) of the EU Charter affirms that

170 B.van der Sloot, 'A new approach to the right to privacy, or how the ECtHR embraced the non-domination principle', in *Computer law &Security Review*, vol. 34, 2018, pp. 539-549.

171 ECtHR, *Malone v. the United Kingdom*, No. 8691/79, 2 Aug. 1984, §. 67; ECtHR, *Rotaru v. Romania*, No.28341/95, 4 May 2000, §.55.

172 *See* 73, § 4.

173 EU network of independent experts on fundamental, *Commentary Of The Charter Of Fundamental Rights Of The European Union*, June 2006, p.95, available at http://www.pedz.uni-mannheim.de/daten/edz-k/gdj/06/network_commentary_final%20_180706.pdf, (accessed the 7th June 2018)

174 European Union Agency for Fundamental Rights, "Handbook on European data protection law", Luxembourg, Publications Office of the European Union, 2014, p. 68, available at http://www.dvi.gov.lv/lv/wp-content/uploads/fra-2014-handbook-data-protection-law_en.pdf , (accessed the 15 June 2018)

limitations on the exercise of the rights and freedoms recognised by the same Charter and, accordingly, on the exercise of the right to the protection of personal data, are admissible only if they:

1) are provided by law; [175]
2) respect the essence of data protection; [176]
3) are necessary, in accordance with the principle of proportionality;
4) meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

Since personal data protection is a distinct and stand-alone fundamental right in the EU legal order, any processing of personal data by itself constitutes an interference with this right. It is immaterial if the personal data in question relate to an individual's private life are sensitive, or whether the data subjects have been inconvenienced in any way. The interference has to comply with all the conditions listed in Article 52 (1) of the Charter. In relation to the existence of an interference with the rights recognised by Articles 7 and 8 of the Charter which could be justified, the ECJ ruled that '*it is common ground that the interference (..) must be regarded as "provided for by law" within the meaning of Article 52(1) of the Charter*'.[177] Articles 1(1) and 2 of Regulation No. 259/2008 expressly provide for such publication'.83 Stated differently, limitations on the fundamental rights recognised by the Charter, which are grounded in a Council Regulation, must be considered as 'provided for by law'. It follows that Article 52(1) of the Charter does not require limitations on fundamental rights to be grounded in an EU measure whose adoption is conditioned upon the European Parliament's co-decision.

2.5 The State obligations concerning the Right to Property.

2.5.1. State obligations according to ECHR.

As it was said in the legal analysis of the discipline of right to property within the ECHR; Article 1 contains three distinct rules: a) the peaceful enjoyment of property; b) the protection against any deprivation of possessions and c) the guarantee concerning the control of the use of property. In

175 This requirement implies that limitations must be based on a legal basis that is adequately accessible and foreseeable and formulated with sufficient precision to enable individuals to understand their obligations and regulate their conduct. The legal basis must also clearly define the scope and manner of the exercise of the power by the competent authorities to protect individuals against arbitrary interference.

176 In the EU legal order, any limitation on the fundamental rights protected under the Charter must respect the essence of those rights. This means that limitations that are so extensive and intrusive so as to devoid a fundamental right of its basic content cannot be justified. If the essence of the right is compromised, the limitation must be considered unlawful, without a need to further assess whether it serves an objective of general interest and satisfies the necessity and proportionality criteria.

177 Court of Justice of the European Union, Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert*, judgment of 9 November 2010, §66.

introducing an analysis focused on the States obligations in relation to the right to property, these three rules must necessarily be considered. For what concerns the first rule, the ECtHR has broadened its scope by declaring that the real and effective exercise of the right of property does not merely impose on the Contracting States a duty not to interfere with such a right, but also imposes a positive obligation to protect it.[178] In the *Öneryildiz V. Turkey*, the Court has affirmed that the obligation arises "*where there is a direct link between the measures which an applicant may legitimately expect from the authorities and the enjoyment of his possession*".[179]

In view of the ECtHR, such positive obligations include the adoption and implementation of measures that are reasonable in each circumstance in order to avoid interferences with the right of property. Following this trend, the heading 'protection of property' was added by Protocol No. 11 to the ECHR and entered into force in 1998. Such addition amounted to an explicit endorsement of an already consolidated jurisprudence of the ECtHR, according to which '*by recognising that everyone has the right to the peaceful enjoyment of his possessions, article 1 of the Protocol 1 is in substance guaranteeing the right of property*'.[180] This protection applies to any measure taken by the public authorities of the contracting States that may interfere with the right with the right to the peaceful enjoyment of one's possessions.[181] According to D.U Fernandez Bermejo, "*such right is conferred to both natural and legal persons, including public law entities as long as they do not exercise governmental powers and can be regarded as non-governmental organisations*."[182]

Article 1 of Protocol No. 1 is the only article of the Convention which expressly mentions "legal persons", and thereby affirms that not only natural person, but also legal persons, may be subject to infringements of their right to property. Every applicant, whether a natural or legal person, must be able to demonstrate the existence of a right to property at issue in order to qualify as a "victim" under the Convention.[183] An applicant can allege a violation of Article 1 of Protocol No. 1 only in so far as the alleged interference relates to his or her "possessions" within the meaning of that provision.[184] Following the Court's case law, and in accordance with the structure of Article 1, it is possible to include the previously mentioned second rule, the protection against any deprivation of possessions, as one of the specific cases of interferences with the right to property. The essence

178 ECtHR, *Öneryildiz V. Turkey*, No. 48939/99, 30 November 2004, §134

179 Ibidem

180 ECtHR, Marckx V. Belgium, No. 6833/74, 13 June 1979, § 63

181 D.U. Fernandez-Bermejo, "The multilevel protection of the right of property in Europe", in "*China-EU Law Journal"*, vol.4, 2015,p.78

182 Ibidem.

183 A. Grgic, Z. Mataga & Others, "*The right to property under the European Convention on Human Rights, A guide to the implementation of the European Convention on Human Rights and its protocols*", Belgium, June 2007, p. 6

184 Ibiden

of deprivation of property is the extinction of legal rights of the owners.[185] The ECtHR has given a narrow interpretation of 'deprivation', by categorizing it as the permanent extinction of the rights of the owner.[186] Therefore, all those legal restrictions that do not amount to a complete removal of ownership, or that constitute temporary or provisional seizures, should not be examined under the second rule of Article 1, but on the basis of the first or third rule.[187]The Court, hence, will be entitled of two specific tasks. On one hand, the Court will consider whether there had been a formal expropriation or transfer of ownership. On the other hand, there will be also investigated the realities of a situation to see whether there has been a *de facto* expropriation.[188] In order to distinguish expropriation from the control of the use of property it is decisive whether a party was able to legitimately expect to continue exercising property rights without any state interference and whether a personal relationship between individual concerned and the property he was deprived of existed.[189]

The third rule introduced by Article 1 of Protocol 1 entails the control of the use of property. A measure can be included in Article 1 of Protocol No. 1 if its main purpose is that the State controls the use of the property, which is in the general interest or "to guarantee the payment of taxes or other contributions or penalties".[190] Thus, this rule applies to those administrative and judicial measures, able to ensure that such properties are used in accordance with the relevant national laws.[191] These measures, as well as it was said previously in talking about the limitations of the right to privacy, must comply with three conditions: lawfulness, justification in a general interest, and proportionality. The Court hence recognizes to the Contracting States a higher degree of discretion the with the previous two rules, by setting the national authorities as the sole judges whether there is or not the necessity for an interference.

185 Ibidem, p. 10

186 See ECtHR, *Handyside v. The United Kingdom*, No.5493/72, 7 December 1976, §. 62; ECtHR, *Erkner and Hofauer v. Austria*, No. 9616/81, 29 September 1987, §74

187 D.U. Fernandez-Bermejo, "The multilevel protection of the right of property in Europe", in "*China-EU Law Journal"*, vol.4, 2015, p.81

188 A. Grgic, Z. Mataga & Others, "*The right to property under the European Convention on Human Rights, A guide to the implementation of the European Convention on Human Rights and its protocols*", Belgium, June 2007, p10. In this context, formal and *de facto* expropriation need to be distinguished. Formal expropriation includes interferences with the right to property on the ground of formal transfer of property. This is, generally, linked with a loss of property for the benefit of the State or in the public interest, and holds true irrespective of whether the expropriation was based on laws, administrative acts or civil law contracts. The expropriation for the benefit of individuals represents, instead, another case of formal expropriation if the grounds for it are set in law or if it is based on acts attributable to the State. On the other hand, *de facto* expropriation doesn't require a formal taking of property. It encompasses authoritative measures whose effects are as seriously adverse as the effect of a formal expropriation.

189 In *Papamichalopoulos v. Greece* the applicants' valuable land had been taken by the State in 1967 during the dictatorship period and given to the Navy, which then established a naval base on the site. Since after that time the applicants were unable to make effective use of their property or to sell it, the State was held liable for a de facto expropriation. See, ECthHR, *Papamichalopoulos v. Greece,* no. 14556/89, 24th June 1993, §. 43 and seq.

190 Grgic, Z. Mataga & Others, "*The right to property under the European Convention on Human Rights, A guide to the implementation of the European Convention on Human Rights and its protocols*", Belgium, June 2007, p. 11

191 D.U. Fernandez-Bermejo, "The multilevel protection of the right of property in Europe", in "*China-EU Law Journal"*, vol.4, 2015, p.83; ECtHR, *Pine Valley Develpments Ltd. and Others v. Ireland*, No. 12742/87, 29 November 1991, § 56

The right to property protection is not, however, an absolute right. Article 1 of Protocol No. 1 clearly mentions the interferences with the right to peaceful enjoyment of possessions. These interferences are allowed only: if they are prescribed by law; if they are in the public interest; and if they are necessary in a democratic society.[192] All three conditions must be fulfilled cumulatively. If only one of them was not respected, there would have been a violation of the Convention. Interference with the right to property must firstly satisfy the requirement of legality. In this sense, the notion of law under the Convention has an autonomous meaning. It is not only a law in a formal sense. Due to the different systems of sources of law in the Member States, justification for legal interferences not always relies on a law adopted in the legislative procedure, but it can also include other legal sources. Any legal interference must be based on an instrument of general application, which must contain certain qualitative characteristics and afford appropriate procedural safeguards so as to ensure protection against arbitrary action. In any case, the legal basis needs to be of a certain quality, namely it must be compatible with the rule of law and it must be sufficiently accessible, precise and foreseeable. The same Court has said that "*the level of foreseeability depends on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed*".[193] Any interference within the individual's property rights may be justified only if it pursues a legitimate aim in the general (public) interest. Under this point of view, States enjoy a wide margin of appreciation in determining what is in the public interest, especially when implementing social and economic policies. The Court, in this sense, will have a broader margin of appreciation in evaluating the "public interest" of these interferences, unless the latter are manifestly without any reasonable foundation. In this sense, measures of deprivation of property are manifestly without reasonable foundation where the implied public interest is not hold genuinely.[194]

Lastly, the principle of proportionality between the means employed and the aim sought to be achieved must always be satisfied. Any measure, which interferes with the peaceful enjoyment of an individual's possession, must necessarily be directed at achieving a legitimate aim, and it must reach a fair balance between the demands of the general interest of the community and the requirements of the individual's fundamental rights.[195] Such a fair balance will not have been struck where the individual property owner is made to bear "an individual and excessive burden". Even under

192 C. Grabenwarter, *supra.*

193 ECtHR, *Sud Fondi S.r.l.a.o.* v. Italy, No. 75909/2001, 10th may 2012, §.109.

194 ECtHR, *Tkachevy v. Russia,* No. 35430/05, 14th February 2012, §.39.

195 Grgic, Z. Mataga & Others, "*The right to property under the European Convention on Human Rights, A guide to the implementation of the European Convention on Human Rights and its protocols*", Belgium, June 2007, p. 14

the evaluation of the proportionality requisite, the Court leaves the Contracting States certain discretion commonly referred to as "margin of appreciation". Given their direct contact with the social process forming their country, States' authorities are considered to be better placed to assess the existence of both the need and the necessity of the possible restriction. In each situation, hence, the Authorities must find a proper balance amongst all the relevant circumstances applicable to the specific case, trying to avoid 'excessive burden'.[196]

On the other hand, the Court shall certainly take into consideration the existence of alternative solutions when ruling whether interference had been proportionated to the aim sought to be achieved. The effective exercise of the right protected by Article 1 of Protocol No. 1 requires positive measures of protection on behalf of the State, particularly where there is a direct link between the measures an applicant may legitimately expect from the Authorities and the effective enjoyment of his possessions.[197] The nature and the extent of these positive obligations for the States Parties varies depending on the circumstances. It is indeed by striking a fair balance between the public interests and the requirements for the protection of the rights that the obligation of adopting positive measures become mandatory.

2.5.2 State Obligations according to EU Charter

As it was previously stated, according to the explanations relating to the Charter, which are to be followed by the Courts of the EU and by the member States when interpreting the Charter, Article 17 CFR is based Article 1 of the Protocol 1.[198] Therefore, as stated by Article 52(3) of the EU Charter, despite the divergences in the wording of both provisions the meaning and scope of the right are the same, and its restrictions may not exceed those provided under Article 1 of the Protocol, while it is possible for EU law to provide a more extensive protection. Thus, what has been said before in reference to Article 1 applies also to Article 17 CFR. As a matter of fact, ECJ has until now interpreted this latter provision in accordance with the aforementioned ECHR provision, and the corresponding case law of the ECtHR, without significant deviations. For instance, it has been established that the protection of the right of property under EU law applies only to existing

196 In this sense, the Courts' case law is very conspicuous: EctHR, *James and* Others v. *UK*, No.8793/79, 21 February 1986, §.46; EctHR, *Katte Klitsche de la Grange* v. Italy, No. 12539/86, 27 October 1994, §§. 42 and seq.; ECtHR, *Spadea and Scalabrino v. Italy*, No. 12868/87, 8 September 1995, §§. 33 and seq. ECtHR, *Urbànska obec Trencianske Biskupice v. Slovakia*, No. 74258/01, 27 November 2007, §§ 120, 132 and seq.

197 D.U. Fernandez-Bermejo, "The multilevel protection of the right of property in Europe", in "*China-EU Law Journal"*, vol.4, 2015, p.80

198 'Explanations relating to the Charter of Fundamental Rights'(14/12/2007), OJ C 303, p7, when it comes to Article 17 it is immediately stated that "*This Article is based on Article 1 of the Protocol to the ECHR'.*, see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007X1214(01)&from=EN, accessed the 6 July 2018.

possession. As well as it was stated in the legal analysis of Article 1 of Protocol 1, there are exceptions to the 'existing possessions rule' under certain conditions. On the one hand, the European Court of Human Rights, and therefore also the ECJ,[199] has accorded the protection to the applicant having a 'legitimate expectation' to collect an asset (receivable). On the other hand, the notion of 'legitimate expectations' has certain limits because both the provisions don't provide a right to become owner (to acquire ownership). 'Legitimate expectations' must be of a nature more concrete than a mere hope and be based on a legal provision or a legal act such as a judicial decision.

2.6 The State obligations concerning the Right to Work.

2.6.1. State obligations according to ECHR.

When it comes to States obligations resulting from the ECHR, it is necessary to remember that within the Conventions there is not a clear and univocal definition about right to work. On the contrary, this right is constructed by using different articles, which have contributed in summarizing four essential elements at the base of this right: livelihood for dignity, non-exploitation, self-realisation and non-domination. Driven by the aim of fulfilling these elements, States obligations descend from three main articles within the ECHR: Article 4 (prohibition of slavery and forced labour), Article 11 (Freedom of assembly and association) and Article 14 (prohibition of discrimination). There is therefore a multilateral system of States (positive and negative) obligations which have to be mentioned in this paragraph.

Moving from the obligations stemming from Article 4, a brief mention must be given to the terms 'forced and compulsory labour'. The Convention, in this sense, doesn't' provide an *ad hoc* definition. Therefore, the Court has interpreted these terms drawing upon international agreements, with a particular reference to the Forced Labour Convention adopted by the International Labour Organisation.[200] According to the Court, forced labour encompasses all forms of personal work, regardless of whether it is of a physical or an intellectual nature, in which the working obligation is not entered into voluntarily.[201] On this very point, the Court has strengthened the duties for the Member States to effectively investigate and punish the perpetrators of acts prohibited by Article 4.

199 ECJ, Case C-283/11, 2013, *Sky O¨sterreich GmbH v. O¨sterreichischer Rundfunk*, 22 January 2013, para. 34: the protection granted by Article 17 CFR does not apply to mere commercial interests or opportunities, the uncertainties of which are part of the very essence of economic activity, but to rights with an asset value creating an established legal position under the legal system, enabling the holder to exercise those rights autonomously and for his benefit.

200 ECtHR, *Siliadin v. France*, No. 733316/01, 26 July 2005, §§. 84, 85 120 and ss.

201 C.Grabenwarter, '*ECHR – A commentary'*, p.55

Concerning the States duties deriving Article 11, they refer to the freedom of association in trade unions. These working associations are able to protect collective interests of the professional categories of works who adhere to them. State interferences with the freedom of association are allowed only if they are prescribed by law. In this sense, the prescription by law require not only an explicit provision within the national law, but also an elevated quality of the law itself, which has to be accessible to the persons concerned and foreseeable to its effects. In the sector of trade unions, in view of the sensitive nature of social and political issues in achieving a balance between the respective interests of workers and administrators, the Member States enjoy a large margin of appreciation. The requisite of proportionality plays hence a pivotal role in these interferences.[202] States have to provide possibilities to freely form an association, by enjoying a wide margin of appreciation in the choice of the means to be employed for forming an association. Moreover, in order to make the right to join a trade union effective, States have to protect individuals against any possible abuse of a dominant position by trade unions. Members States are obliged to secure the effective enjoyment of freedom to join trade unions. States must also guarantee that no negative consequences will arise for an employee due his/her membership of a trade union.

Lastly, Member States have to comply with the obligations arising from Article 14 on the prohibition of discrimination. Discrimination, within the meaning of Article 14, presupposes that individuals, placed in analogous or relevantly similar situations, are discriminated in the enjoyment of their Convention rights and freedoms. In order to prove that a violation has occurred, it has to be first demonstrated that similar situations were treated differently. The right not to be discriminated against is also violated if States, without objective and/or reasonable justification, fail to treat differently persons whose situation are significantly different.[203] Despite positive obligations aren't expressly mentioned within Article 14, it is still possible to deduce them *a contrario.* In this sense, the prohibition of discrimination could be read as the State obligation in providing equal treatments to all its citizens. The Court has also derived some positive obligations by the conjunct reading of Article 14 and 11. In the case *Danilenkov and others vs. Russia,* for instance, the Court has required to the State to "*adopt effective and clear judicial protection against discriminations on the grounds of trade union membership*".[204]

202 However, where a principle defended by a trade union is not at variance with the principles of democracy and there are no signs of incitement to resort to violence, proceedings to dissolve a trade union are not proportionate.

203 ECtHR, *Thlimmenos v. Greece*, No. 34369/97, 6th April 2000, § 44; ECtHR, *Pretty v. UK,* No. 2346/02, 29 April 2002, §§ 88 et seq.; ECtHR, *Angelova and Iliev v. Bulgaria,* No. 55523/00, 26 July 2007, §.117.

204 ECtHr, *Danilenkov a.o. v. Russia, No.* 67336/01, 30 July 2009, §76

2.6.2 States obligations according to EU Charter.

It must be recalled that Article 15 §. 1 doesn't mention the "right to work" in general, but it specifically refers to the "right to engage in work". In this sense, Article 15 has introduced the right to have the opportunity to work. The right to work was not included in the EU Charter because of possible repercussions on the balance of powers and competences between the EU and its member states. The "right to engage in work" focuses on employability, reflecting a declared goal of the EU.

Article 15, however, should not be read in the sense that introduces an obligation of the State to provide everyone with paid employment, nor the right to demand work. Rather, this right must be conceived as an individual freedom involving the free choice of work, but also the possibility of gainful employment. Article 15 *de facto* reinstates the provisions of Article 1 (2) of the European Social Charter,[205] by the acceptance of which the Parties have undertaken to protect effectively the right of the worker to earn his living by work freely undertaken. The European Committee of Social Rights considers that this clause has two effects: it prohibits forced labour and lays down the principle of the prohibition of any discrimination in access to employment. With regard to this latter aspect, the Committee is of the opinion that the prohibited acts and discriminatory provisions are all those which may occur during recruitment and in the conditions of employment in general (mainly: remuneration, training, promotion, transfer, dismissal and other prejudice). In particular, it is for States to take legal measures to ensure the effectiveness of the prohibition of discrimination. These measures consist at least of:

- that any provision contrary to the principle of equal treatment contained in the collective labour agreements, the employment contracts and the internal regulations of enterprises may be declared void or be rejected, withdrawn, repealed or amended;
- that adequate and effective remedies are available in cases of alleged discrimination;
- to give adequate protection against dismissal or other reprisals by the employer against the employee who has lodged a complaint or brought legal action;

205 European Social Charter, Article 1: "

- that in the event of a violation of the prohibition of discrimination, sanctions should be sufficiently dissuasive for the employer as well as adequate and proportionate compensation for the injury suffered by the victims.

States have two positive obligations: on one hand, States must all those positive legal measures able to ensure the effective and peaceful enjoyment of engaging in a working activity. More specifically, these measures aim in removing the concrete obstacles for the individuals who wants to engage in a paid employment and in disciplining all the aspects – such as working hours, working conditions, minimum wages – the absence of which may severely preclude or restrict the effective enjoyment of these rights. At the same time, States are obliged in removing all the possible factors which may lead to discrimination on the ground of the work.

In many judgments, the European Court of Justice has emphasized the direct effect of the freedom of establishment[206] and the freedom to provide services.[207] She interpreted these basic community freedoms in the light of human rights. The ECJ ruled that, "*although it is true that guarantees are granted in the constitutional order of several Member States for the free exercise of professional activities, the right so guaranteed, far from being an absolute prerogative, must also be considered in view of the social function of protected activities*."[208] It noted that in this case the Community measure in no way affects access to the profession or the free exercise of this profession.[209]

PART III

- AN ANALYSIS ON THE CONCRETE ISSUES FACED BY RIGHT-HOLDERS AND DUTY-BEARERS THE ENJOYMENT AND THE PROTECTION OF THE RIGHTS WITHIN THE BITCOIN NETWORK -

2.7 From whom these problems can be addressed?

The third part of this chapter will focus on the issues that occur in the enjoyment and exercise of the rights previously analysed in relation to the bitcoin network and blockchain technology. Bitcoin phenomenon, given its innovative technological and cultural scope, has raised doubts whether the exercise of certain rights, strictly related to the human beings' personal realisation, could be valid even within a digital world. Before proceeding to check which are the main problems, it has to be clarified who may face issues in exercising its rights. Namely, who are right-

206 Court of Justice of the European Union., *Reyners*, No. 2/74, 21 June 1974, p. 631.

207 Court of Justice of the European Union, *Van Binsbergen*, No. 33/74, 3 December 1974, p. 129

208 Court of Justice of the European Union, *Nold c. Commission*, No. 4/73,14 May 1974, p. 491, points 13 et 14.

209 Ibidem.

holders in the bitcoin network. Although at the moment it is possible to identify an extensive list of potential Bitcoin actors, not all of them necessarily need to be regulated. The more probable addressees for regulation are the following:

1) *Users*: according to the European Banking Authority (EBA), "*a user is a person or legal entity that obtains bitcoins and uses it to purchase real or virtual goods or services, or to send remittances in a personal capacity to another person (for personal use), or who hold the bitcoins for other purposes, such as an investment*".[210]

This broad definition embraces then all those subjects who are in possess of a certain number of bitcoins. For the purpose of this introduction -identifying all the right holders involved in the network and affected by the blockchain technology - two further categories of individuals must be taken in exam. Even though they are owners of bitcoins, and therefore they could fall within the definition of bitcoin user, the reasons behind the ownership help to distinguish them from each other. It is therefore possible to configure the following categories of subjects:

1a.) *Investors*: investors are those who have decided to buy huge amounts of bitcoins, with the aim of obtaining a profit, hoping in this sense in an increase of the monetary value of bitcoins.

1b). *Miners*: miners are those who solve complex algorithms to obtain small amounts of bitcoin. Miners tend to operate anonymously, from anywhere in the world, and validate bitcoins' transaction, which will be inscribed within the blockchain ledger. Miners have hence the pivotal role of checking the validity of the transactions, ensuring the resilience and the well-functioning of the whole Bitcoin network.

2) *Exchangers*: an exchanger is a person or entity engaged in the exchange of bitcoins for fiat currencies. "They may generally accept a wide range of payments, including cash, credit transfers, credit cards and also other cryptocurrencies".[211] Exchangers oftentimes act as the "seller" of the convertible virtual currency and the user functions as the "purchaser".

3) *Legal and business consultants*: this category of subjects deals with providing new potential bitcoin users - both the users in a broad sense, and as well investors and miners - all

210 EBA, *'Opinion on 'virtual currencies'*, 4 July 2014, p. 13-14 purchased at https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

211 FATF Report, "Virtual Currencies Key Definitions and Potential AML/CFT Risks", June 2014, p. 7 available at http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (accessed the 15 June 2018)

the legal and commercial information aimed at filling any knowledge gaps and limiting consequent economic losses.

Bearing in mind these categories of right holders, the analysis of this chapter will start by taking into account the three human rights selected for this work. In the analysis that will be carried out for each human right chosen, a first part will indicate the positive aspects that the bitcoin network and blockchain technology has in exercising these rights. Subsequently, the main problems will be indicated, highlighting the legal gaps in this regard. This will be done in order to introduce the third part of this work, concerning the approaches that should be used in order to minimize any violation of these rights.

2.8. The issues faced in relation to the Right to Privacy

As it was described within the first part of this chapter, the conception of the right to privacy, within the European legal framework, has seen a constant evolution, adapting itself to new challenges - both cultural and technological - that could have limited (or broadened) its purpose and its primary function. Moving from the four different spheres just broadly listed in Article 8 ECHR and Article 7 of the EU Charter, through the introduction of the concept of 'data protection' it was enlightened the constant evolution of privacy, in tandem with the evolution of the surrounding environment. The recently adopted GDPR, furthermore, has shown a tendency to give individuals an increasing control over the protection of their data, particularly in the context of the Internet, where data belonging to an individual can circulate freely and without his/her direct control. Contextualizing Bitcoin phenomenon and blockchain technology within the already existing legal framework is undoubtedly a very hard task. These two technological and cultural innovations can have, both positive and negative impacts for what concerns the right to privacy.

In considering the positive insights, these two technologies can have a helpful impact in terms of increasing individuals' control over their privacy, following, in this sense, the recent European regulation. This increased control could be achieved thanks to three key factors: the decentralized system, the high level of transparency and the encryption and pseudonymization techniques. The decentralized nature of the whole Bitcoin network can be applied within the broader scope of decentralization as a response to the growing centralizing nature of the Internet. The Internet, in fact, was originally conceived as a distributed network of networks. In contrast to its original purpose, Internet has turned down into a new space for power centralization and control, due the high level of digital surveillance, which has contributed to the widespread belief that the internet is a 'control

technology'.[212] Central platforms within Internet collect, by design, information about users' online activities. In this context, personal data represent a core aspect within digital economy, contributing in increasing the power of those who, legitimately or not, exercise their control by profiting of an in-depth knowledge of customers' trends and behaviours. The decentralized nature of Bitcoin ensures two great accomplishments to the peers operating within the network. First, the lack of a central party with an extended control over individuals' data from storing and processing activities gives to the users the concrete perception of not having to fear to be secretly controlled. Secondly, thanks to this freedom, any possible type of profiling of a user by a third (more or less centralized) party becomes almost impossible. Moreover, thanks to the high resiliency of the blockchain technology, the susceptibility to attacks from third parties is severely reduced. The distributed nature of the blockchain ledger provides an higher security level in preventing data tampering and computer's failure. The system is also made incorruptible due the irreversibility character of blockchain, since any change of block would affect all the others in the chain and this incompatibility will reveal a malicious attempt.[213]

Another key factor which contributes in the huge trust users have towards Bitcoin and blockchain technology is its transparency. Within the blockchain ledger, which is an open source, participants know what data are collected about them and how they are processed.[214] With the concrete example of Bitcoin, the blockchain ledger used within the Bitcoin network shows all the bitcoin transactions operated by the users, the amount of bitcoin transferred from one user to another and when the transaction was realized. Blockchain technology has aroused interest thanks to a shared, distributed and fault-tolerant data base. Each participant in the network can share his ability to neutralize opponents by exploiting the computational skills of honest nodes and the information exchanged is resistant to manipulation. This is due not only to the transparency of the ledger, but also to the transparency of the blockchain protocol. Since users do not have to trust third parties for managing the software, it is evident that blockchain strengthens users' autonomy and control over platforms' activities and processing data.[215]

212 M. Castells, "*The Internet Galaxy: Reflections on the Internet, Business and Society",* Oxford University Press, London, 2001 cited by 212 R. Filippone, "Blockchain and individuals' control over personal data in European data protection law", Master Thesis, Tilburg University, August 2017, p.5 available at http://arno.uvt.nl/show.cgi?fid=143638 (accessed the 10 June 2018)

213 N. Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, in *Telecommunications Policy*, 2017, vol. 41, pp. 1027-1038, purchased at https://acelscdncom.uaccess.univie.ac.at/S0308596117302483/1-s2.0-S0308596117302483-main.pdf?_tid=87610b2b-23a2-41c8-8348-87f20c5935aa&acdnat=1529909137_af87b6dee1ba12da0a5250fc746efb4e, (accessed 16th June 2018)

214 R. Filippone, "*Blockchain and individuals' control over personal data in European data protection law*", Master Thesis, Tilburg University, August 2017, p.29 available at http://arno.uvt.nl/show.cgi?fid=143638 (accessed the 18 June 2018)

215 Ibidem

The privacy of the users within the Bitcoin network is also granted by the combination of an end-to-end encryption of the communication, requiring a private and a public key, together with the pseudonimity of the same users. Despite the transparency of the ledger, the crypto-numerical pseudonimity granted by the public key of a bitcoin wallet ensures *de facto* the users' almost absolute anonymity. Anonymity is probably one of the properties that has contributed to the success of bitcoin deployment., based also on the fact that users can create any number of anonymous bitcoin addresses that will be used in their bitcoin transactions.[216] Unless Bitcoin users publicize their wallet addresses publicly, it is extremely hard to trace transactions back to them. However, even if the wallet address was publicized, a new wallet address can be easily generated. If compared to traditional currency systems, where third parties potentially have access to personal financial data, it appears obvious that this kind of system enhances users' privacy. Moreover, as it was correctly pointed out by M. Conti, "*this high anonymity is achieved without sacrificing the system transparency as all the bitcoin transactions are documented in a public ledger*".[217]

If on one hand the Bitcoin phenomenon and the blockchain technology may appear as a privacy-enhancing architecture, on the other hand factors as the ledger's irreversibility, its transparency and also the same pseudonimity may negatively affect users' privacy. As already mentioned in paragraph, blockchain technology can have several different applications in several areas, such as for the registration of certificates, or for engaging in economic transaction, or to order medical prescription.[218] The problem arises when a transaction is registered within the blockchain ledger: since it is impossible to remove from the record from the ledger, anyone can see specific details that someone may have a legitimate interest in having it removed or modified.[219] Deleting a determined information from the block-chain ledger could be possible only if the 50% +1 of all the nodes operating in the network cooperate in order to rebuild the chain of blocks since data were added. Meanwhile this time-consuming operation is carried out new transactions can't be validated. In these particular situations, the exercise of individuals' right to be forgotten, according to article 17 GDPR, is *de facto* impossible.

216 J. Herrera-Joancomartì & C. Perez - Solà, "Privacy in Bitcoin Transactions: New Challenges from Blockchain Scalability Solutions", in *Modelling Decisions for Artificial Intelligence*, 2016, pp. 26-44, p. 38, available at https://link-springer-com.uaccess.univie.ac.at/content/pdf/10.1007%2F978-3-319-45656-0.pdf, (accessed the 19 June 2018)

217 M. Conti, "A Survey on Security and Privacy Issues of Bitcoin", in *IEEE Communications Surveys & Tutorials*, available at https://arxiv.org/pdf/1706.00916.pdf (accessed the 20June 2018)

218 S. Ølnes, J. Ubacht & M.Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing", in *Government Information Quarterly*, 2017, Volume 34, Issue 3, Pages 355-364.

219 See. R. Filippone, p. 30

Another key issue within the whole Bitcoin and blockchain technology is directly linked to the transparency of the ledger, and its association with the double-spending solution. In order to check the validity of transactions, nodes are entitled to access to all the previous transactions relating to the parties involved. This implies that nodes need to trace the full financial history of a particular wallet associated to an actor. This visibility of all the interactions occurred in the blockchain is clearly intrusive for the privacy of the people involved, even more so considering that the public blockchain is open to anyone in the world.[220] These interactions amongst peers are in open contrast with the principles of data minimization and storage limitation, which were two of the cardinal principles behind the adoption of the GDPR. This is valid even for what concerns the pseudonimity of the peers, since their data remain still visible in the public ledger allowing to trace the operations carried out by the users. The pseudonymized data according to Article 4(5) GDPR are still relating to an identifiable natural person. In this sense, pseudonymisation merely prevents the attribution of these data to a natural person. In other words, GDPR pseudonymisation prevents direct identification through attribution, but not through any other means reasonably likely to be used to identify an individual, which must be excluded before he or she is no longer considered to be identifiable. The combination of metadata's transparency, users' identifiability and immutability of the chain can represent a dangerous mixture for the users' privacy. This problem raises the already discussed debate about the extent to which an interference of the state in an individual's privacy can be considered legitimate or not.

These privacy risks affect principles and rights recognized and protected both by Article 8 of the EU Charter of Fundamental Rights and, foremost, by the GDPR. The recent European Regulation which finds its application due to the processing of personal data and their storing within the blockchain ledger. As a counterbalance for the lack of a central trusted party, an higher level of coordination among peers of the network is therefore required. This is achievable by making data – more specifically metadata, which can also be personal data - available to the participants through the distributed and public ledger of the blockchain. From this point of view, it is possible to apply Article 4 of the GDPR, according to which "*personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors […].*"

220 Ibidem

In addition, even in the Preambles of GDPR is set forth that "*data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person*."[221] Therefore, pseudonimity only makes it harder to identify the data subject, but not impossible.[222] It follows that the information shared in the blockchain can be qualified as personal data and, therefore, the GDPR applies. Pseudonymisation, within the meaning of GDPR Article 4(5) and Recital 26, would be inadequate to address all of the risks of identification encompassed within the 'means reasonably likely to be used' test. Although recital 26 GDPR considers pseudonymised data to be personal as long as there is additional information kept separately and secure within a key, the pseudonymisation needs to be regarded within its effect towards the third party not holding the key. In order to grant an appropriate legal assessment, the characteristic of the specific data shall be determined from each point of view of the specific party concerned, with the consequence that the same pseudonymous data-set is personal for the key-holder but may be anonymous for a third party other than the key-holder. Hence, pseudonymisation may lead to render data anonymous depending on the special situation and depending on the view of the certain person concerned who is processing the pseudonymised data.[223]

Furthermore, the architecture of blockchain stands in open contrast to the GDPR at its very foundations. While GDPR's obligations are conceived for centralized architectures, characterized by clear distribution of role, blockchain's peer-to-peer technology is instead featured by distributed community and fragmented actions.[224] The peer-to-peer design openly questions the application of traditional legal regulation and opens the debate on the subjects who are required to observe the GDPR. Furthermore, it reinforces doubts about who should be held responsible for the processing and protection of personal data through the implementation of appropriate technical and organizational measures according to the principle of responsibility, as required by Article 5 of the GDPR.[225] A second point of contention between blockchain and GDPR is when we refer to the principle of data minimization. According to Article 5 (c), GDPR, data processing should be "*adequate, relevant and limited to what is necessary in relation to the objectives for which they are processed*".[226] Because of the only-additional feature of blockchain, the amount of personal data

221 Recital 26 GDPR.

222 R. Filippone, "*Blockchain and individuals' control over personal data in European data protection law*", Master Thesis, Tilburg University, August 2017, p. 32

223 M.Karg, "Anonymität, Pseudonyme und Personenbezug revisited?," in *Datenschutz und Datensicherheit (DuD,*) Vol.39, 2015, Issue 8, pp. 520-526

224 Supra, n. 218

225 R. Filippone, "*Blockchain and individuals' control over personal data in European data protection law*", Master Thesis, Tilburg University, August 2017, p.32

226 Article 5, (c), GDPR

shared in the blockchain can only increase block after block creating, in this sense, a redundancy of data.

Also the immutability of the ledger, one of the main characteristics of the blockchain, is in stark contrast to the specific rights introduced by GDPR. In this sense, the exercise of the rights *to rectification* (Art. 16, GDPR) and the right "right to be forgotten" (Art. 17, GDPR) see their absolute inapplicability due to the blockchain's technical features. The right to be forgotten is one of the most important innovations operated by GDPR, and it needs to be balanced against other interests, such as the interest of third parties in conducting business. But, in a system in which everyone has a direct access to others' information, this become impossible and therefore this right is impossible to be achieved and sufficiently protected.

In conclusion, if the "who", the identity of the users, is hided within the system, on the contrary the "what", the content of the communications, expressly disciplined both by Article 8 ECHR and Article 7 EU Charter, can be openly consulted by anyone. It is therefore evident that the blockchain technology and, so far, the whole Bitcoin network don't comply with the recently updated European data protection law. The specific risks of this legal impasse may imply that individuals, even though on the basis of GDPR get more control over their personal data, will be ultimately more vulnerable. If not combined with appropriate safeguards, the innovative features of immutability, transparency and distribution will turn into critical innovations for Bitcoin's users. If not regulated, blockchain may replicate what has happened with the Internet that from a decentralized space has turned into a centralized one in the hands of powerful corporations.[227] At its worst, it could become a new version of the panoptic, a distributed one where the controllers are those who know the code. Under this point of view, probably it would certainly have been appropriate for the GDPR developers to introduce some specific rules aiming to regulate (or at least superficially touching) the scope and uses of blockchain technology.

2.9 The issues faced in relation to the Right to Property

Despite, as it was stated in paragraph 2.2.1, one of the major problems concerning right to property is give a univocal definition to the right to property - due its strict relation with the national legal provisions of each State- the steps forward realized by the European legal frameworks, have had

227 R. Filippone, "*Blockchain and individuals' control over personal data in European data protection law*", Master Thesis, Tilburg University, August 2017, p.29

the great merit of reducing these discrepancies amongst Member States legislations. A key element which stands out after the previously performed comparative analysis is the principle of 'peaceful enjoyment of property'. In providing that, both the ECHR and the EU Charter of Fundamental Rights have shown their commitment in protecting the inner essence of the right to property. The introduction of this key concept has allowed the Court of Strasbourg to present, expand and substantiate the right from a potentially limited understanding under national law, by encompassing private law notions of possessions and ownership, and recognising legal persons as right-holders.[228] In clarifying that the right to property is *de facto* guaranteed by the possession,[229] the ECtHR has also specified that *"(...) possession is not limited to ownership of physical goods and is independent from the formal classification in domestic law: certain other rights and interests constituting assets can also be regarded as 'property rights', and thus as 'possessions' for the purposes of this provision*".[230] The Court has determined that possession does not include the mere ownership of immovables, but also ownership of shares, entitlements to pension and rent, as well as rights arising from debts. The element of debts become very important when it comes to 'bank money'. 'Bank money', or incorporeal money, is the term economists have used to describe balances held by costumers in banking institutions, which as a chose in action is a debt owing by the bank to its customers.[231] From this point of view, bitcoins are very similar to the concept of 'incorporeal money' used in the economic sector. Moreover, in the economic field, the concept of right to property embraces a whole '*bundle of rights'*, which will be useful in linking the right to property with the bitcoins' possession. This 'bundle of rights', explained by Daniel Klein and John Robinson, encompasses mainly four different rights: "*the right to use the good, the right to earn incomes from the good, the right to transfer the good to others and the right to enforce property rights*".[232]

There are numerous intrinsic characteristics of bitcoins that can fall within the concept of right to property (understood both in the legalistic and the economistic terms). Bitcoins' immateriality and their 'stocking' within bitcoins' wallets can be associated, in a broader sense, to the concept of 'bank money' and to the subsequent rights granted to customers towards their banks. At the same time, bitcoins' potential use both as a medium of exchange, unit of account and as a reserve of

228 J.H. Dalhuisen, 'Legal Orders and Their Manifestation: The Operation of the International Commercial and Financial Legal Order and Its Lex Mercatoria', in *Berkley Journal of International Law,* 2006, vol. 24, pp. 129-141.

229 ECtHR, Case of *Marckx v Belgium*

230 ECtHR, *Case of Beyeler v Italy*, No 33202/96, 5 January 2000, par.100.

231 K.F.K. Low & G.S.Teo, "Bitcoins and other cryptocurrencies as property?", in *Law, Innovation and Technology,* vol. 9, no. 2, 2017, p.242 .

232 D.B.Klein and J. Robinson, 'Property: A Bundle of Rights?', in *Econ Journal Watch,* September 2011, vol. 8, number 3, pp.193-204

value, as well as the possibility of trading bitcoins (or bitcoins' fractions) to other peers, allows to exercise the rights included in the bundle of rights. Generally speaking, ownership of bitcoin is established through successful completion and recordation of transactions on the bitcoin block-chain.[233] Once a transaction is deemed to be valid by users, it will be included in a subsequent block of transactions on the blockchain, rendering it effectively irreversible and enforceable against third parties.[234] It is in this way that the 'peaceful enjoyment of the right to property' is legitimately used by a bitcoin owner.

Nevertheless, it is evident that trying to reconduct the possession of bitcoin within the legal provision of Article 1 of Protocol 1 and Article 17 it's a task which presents numerous issues. The first issue has to traced back to the *unmaterial* nature of bitcoin. Bitcoins differ from coins and bank-notes since the is no fungible thing able to comprise a bitcoin.[235] It could be argued that if at all bitcoins can be considered property, it must be tangible. This is a narrow view of 'property', closely aligned with the aforementioned Birksian distinction between rights *in rem* and rights *in personam*, and it risks to lead to a methodological mistake. The reasoning according to which the absence of a physical thing (in the present case bitcoins) leads to the incapability of owning is legally inconceivable. Whilst it is clear that bitcoins are intangible, it is also clear that they are distinguishable from bank money and incorporeal money.[236] The right to property is, in these particular circumstances, exercised with different premises. Bank money is derived from fiat currencies, under the form of a debt. The debtor/obligor is the bank, which is the so-called 'trusted third party' to which Nakamoto refers in his paper.[237] Bitcoins, instead, by relying on a system without trusted third parties, can't take the form of a debt obligation, given the absence of a 'debtor subject' and of the double-spending possibility.

The lack of a central authority introduces the second issue: Bitcoin system's security. If, on one hand, the lack of a trusted third party gives much freedom to the users, on the other hand it doesn't protect at all the user in the case of bitcoins' theft. A central authority – which, broadly speaking, can be a State authority or, more specifically, a bank institute- has the duty of guaranteeing the security of an individual's property by any possible interference from other individuals. Within

233 J. Dax Hansen & J.L. Boehm, *"Treatment of Bitcoin Under U.S. Property Law"*, March 2017, p.5, available at https://www.virtualcurrencyreport.com/wp-content/uploads/sites/13/2017/03/2016_ALL_Property-Law-Bitcoin_onesheet.pdf, (accessed the 3 July 2018)

234 Ibidem

235 K.F.K. Low & G.S.Teo, "Bitcoins and other cryptocurrencies as property?", in *Law, Innovation and Technology*, vol. 9, no. 2, 2017, p.245

236 Ibidem, p. 246

237 K.F.K. Low & G.S.Teo, "Bitcoins and other cryptocurrencies as property?", in *Law, Innovation and Technology*, vol. 9, no. 2, 2017, p.246

Bitcoin network the subjects entitled of these tasks are the same users. Users of bitcoins are vulnerable at several levels. Some of these vulnerabilities are theoretical. Others, instead, have already been exploited. The most known theoretical example is if a person or more likely group of persons gains control of more than 50% + 1 of the total network hash power of the bitcoin network, they can invalidate transactions and/or double spend bitcoins from their own bitcoin addresses. It is very unlikely that an attack may occur. There are several reasons why this will not happen. "First, it is extremely expensive to amass sufficient computing power to launch such an attack. Secondly, such an attack will lead to widespread reluctance to accept bitcoins as payment, causing its value to plummet; a counterproductive effect for persons controlling sufficient nodes to launch such an attack as they are likely to hold a lot of bitcoins".[238] Users of virtual currencies could be exposed to risks associated with the growth of a virtual currency. For instance, if a closed scheme virtual currency would develop into a unidirectional or even a bidirectional virtual currency, the user of such virtual currency would be exposed to risks that would not have been present initially.[239] For investors, these risks apply as well. Moreover, investors are particularly exposed to the volatility of cryptocurrencies, which may affect the value of their economic investments.

A more concrete vulnerability for a user is the theft of the private key. If it is stored electronically on his personal computer or mobile device, this 'theft' or hack can be achieved using malicious e-mail attachments or applications or by using keystroke logging devices or software to trace the private cryptographic key as it is typed in.[240] If a wallet is used to store the private cryptographic key, then any password used to secure access to the wallet may be hacked. Even if the private cryptographic key is not stored electronically but offline, for example using a so-called paper wallet, access to the private cryptographic key will still allow a 'thief' to make off with one's bitcoins.[241] These risks are exacerbated by the risks of loss of value through loss of the private key, which translates to a need to back it up.[242]

238 On this point, J. A. Kroll, I.C Davey and E. W Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries", in '*The Twelfth Workshop on the Economics of Information Security*', Washington DC, 11-12 June 2013, pp. 11-12; K.F.K.Low, and E.Teo, 'Legal risks of owning cryptocurrencies', in *Handbook of Digital Finance and Financial Inclusion*, 2017, Vol 1, pp.225-248; K.F.K. Low & G.S.Teo, "Bitcoins and other cryptocurrencies as property?", in *Law, Innovation and Technology*, vol. 9, no. 2, 2017, p.250

239 C. Thorpe, J. Hammer, J. Camp, J. Callas and M. Bond, 'Virtual Economies: Threats and Risks'. in: Dietrich S., Dhamija R. (eds) "*Financial Cryptography and Data Security*". FC 2007. Lecture Notes in Computer Science, vol 4886. Springer, Berlin, Heidelberg

240 K.F.K.Low, and E.Teo, 'Legal risks of owning cryptocurrencies', in *Handbook of Digital Finance and Financial Inclusion*, 2017, Vol 1, pp.242

241 This happened to the CEO of a financial services company who left his account information in his car while having it valet parked, see E.Maras "Researcher Has Bitcoin Stolen off His Back in a Public Experiment", in *Crypto Coins News*, 11 November 2015, https://www.cryptocoinsnews.com/researcher-bitcoin-stolenoff-back-public-experiment/, Retrieved 6 July 2018.

242 K.F.K. Low & G.S.Teo, "Bitcoins and other cryptocurrencies as property?", in *Law, Innovation and Technology*, vol. 9, no. 2, 2017, p.250

In correlation to the negative consequences that these risks may have on an individual's 'peaceful enjoyment of property', it has been developing a second current of thought on the relation between bitcoins and property rights. According to this theory, the true right to property is not exercised in relation to the possession of bitcoins, but rather over the private key. Through the ownership of the private key, it is possible to access to the bitcoin wallet, and therefore to exercise the rights connected to the 'presence' of bitcoins within the wallet. As it was pointed out by Adrianne Jeffries, '*if you own bitcoins, what you actually own is the private cryptographic key to unlock a specific address'*.[243] From the assumption of conceptualising property of bitcoins as property of the private key, two possible conclusions could be deducted. As a first consequence of this assumption, the right to property over the private key falls entirely outside the scope of Article 1 ECHR and Article 17 EU Charter. The two dispositions, in fact, don't provide a specific discipline over an individual's confidential information. Secondly, it is possible to narrow the scope of control over the information that comprises the private cryptographic key in order to avoid public policies concerns over 'propertising' information.[244]Instead of granting a larger and more diffused control over use of the private keys, the right exercisable above private cryptographic key would instead be conceived as *'the right to use the key to carry out the "transfer" from the corresponding specific public bitcoins*'.[245] According to this view then, an eventual theft of the private key would be configurable more as a '*cybercrime'*, as disciplined by the EU Directive 2013/40,[246] instead of a normal theft of a possession. This Directive has introduced a whole new series of obligations for the Member States, which have to introduce all those measures able to prevent the widespread of these cybercrimes.

Regardless of whether bitcoins or private keys should be considered to be subject to the right to property, it is possible here to make some considerations. The bitcoins' mania has led to much regulatory attention and thus, understandably, much of the legal analysis of bitcoins has focused on its regulation. Much less attention has been focused on how the private law might deal with bitcoin 'ownership'.

2.10 The issues faced in relation to the Right to Work

243 A.Jeffries, 'How to steal Bitcoin in three easy steps', *The Verge*,19 december 2013, https://www.theverge.com/2013/12/19/5183356/how-to-steal-bitcoin-in-three-easy-steps, accessed the 6th July 2018.

244 K.F.K. Low & G.S.Teo, "Bitcoins and other cryptocurrencies as property?", in *Law, Innovation and Technology*, vol. 9, no. 2, 2017, p. 248

245 Ibidem

246 EU Directive 40/2013 'on attacks against information systems and replacing Council Framework Decision 2005/222/JHA'. In defining the illegal access to information systems, Article 3 of the Directive says: "Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor."

In referring to the issues related to the exercise of the right to work in Bitcoin network and using blockchain technology, a first, important distinction has to made immediately. Within the bitcoin phenomenon, there are two types of work activities: those activities, such as the *mining* activity, which are entirely carried out 'within' the network; and those activities, such as providing exchange services between virtual currencies and fiat currencies, or legal and commercial advices for those who want to invest in bitcoins, which are realized 'outside' the network. The major risks in the both the working activities are connected with a lack of adequate legislation. While the activities realized 'outside' the network have recently seen a first, important step made by the European legislator in regulating their legal position, in particular for what concerns the exchangers of bitcoins, nothing has been done with regard to the *mining* activity.

The key elements that have been identified previously in the analysis of the right to work within the ECHR and the EU Charter can perfectly fit into the mining activity, thus configuring it as a fully-fledged valid work. Through *mining*, it is possible to earn profits able to fulfil not only the self-realization of a *miner*, but also to provide good livelihoods for living – even by considering of the high costs in running this kind of activity.[247] Moreover, new 'associations of miners', the so-called 'mining-pools'[248] are rising up: initially, individual operators were able to carry out this activity on their own. Today, due the increasingly difficulty in accomplishing the extraction of Bitcoin, advanced and complex computing skills are required, and only by combining the powerful hardware systems of these new mining pools groups it could be possible to remain competitive in the *mining* market. This labour market is also characterized by the absence of exploitation of the work. Thanks to the 'proof of work' mechanism, there is an automatic compensation of the computational work carried out by each miner. In this type of market it must be noted an extreme valorisation of the work, in addition to an evident meritocracy, which rewards the speed and perfection in the achievement of data results.

Nevertheless, *mining* presents a series of practical problematics which make *de facto* its legal regulation in the labour market a very complicated task. The first remarkable problem is that the core of the whole *mining* job it's carried out by computers, and not by humans. It follows that attempting to report labour regulations, especially those related to working conditions and/or working hours, to mining, appears to be very complex, because of the inherently human application of these

247 Creating cryptocurrencies requires a high computing power and consequently a high energy expenditure, which makes mining often unsuccessful for individual operators. According to some estimates, the total electricity used annually to produce Bitcoin in fact exceeds 32 terawatts, therefore well above the consumption of a country like Ireland (25 terawatt a year).

248 See paragraph 1.3.3

norms. Secondly, due to its solely electronic nature, it is not even possible to apply those contractual rules, able to regulate the different aspects of a work performance. This lack of regulation affects miners' right to work from being fully exercised and enjoyed. Under this point of view, *miners* – and therefore *mining*- are workers in a condition of so-called 'legislative precariousness',[249] namely a vulnerability created or exacerbated by law. This precariousness can also be seen as a form of discrimination towards miners who, in case of violations of their rights (i.e., in subscribing to a mining pool, the fees are too high, consequently reducing the profit margin), can't complain against any court.

On the other side, when it comes to the providers engaged in exchange services between virtual currencies and fiat currencies and those offering legal and commercial advices for possible bitcoin investors, the situation is different. These two categories, although their working activities present the innovative element of bitcoins, are already regulated within the legal systems both national and European. Moreover, the exchangers of virtual currencies have recently found legal cover thanks to the EU Directive 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.[250] For service providers, one risk is that new regulation may impede their business model or impose requirements which can be unattainable for the smaller ones. This could push smaller service providers out of the market or limit market access. Second, service providers who are not the issuer of a virtual currency may become dependent on that issuer. The issuer may implement substantial changes or may even end the scheme. In the case of cryptocurrencies, where there is no central issuer, there is a clear dependency on miners to validate transactions. These miners could collude to raise transaction fees, thus impeding the development of other service providers. Another risk which may affect exchangers is, according to EBA, that 'they become unable to fulfil payment obligations denominated in Bitcoin or fiat currencies.'[251] This risk affects the exchange and, consequently, also affects its creditors, because the exchange lacks adequate governance arrangements to oversee transactions, fails to keep adequate records, or possesses inadequate funds to repay creditors. Moreover, always according to EBA, there is the risk that the '*protocol that controls a particular virtual currency could be technologically faulty or compromised, or the IT environment at the exchange itself could lack reliability or*

249 V. Mantouvalou, The Protection of the Right to Works Through the ECHR, in *Cambridge Yearbook of European Legal Studies*, vol. *16*, 2012, pp. 313-332,

250 EU DIRECTIVE 2018/843, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN, accessed the 10/07/2018.

251 EBA, *'Opinion on 'virtual currencies'*, 4 July 2014, p. 30 purchased at https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

security'.[252] This situation may damage the activity of an exchanger, who could not hold accountable for such inefficiencies.

2.11 The challenges for a Bitcoin regulation. The issue of the self-enforceability of Bitcoin Network.

It has been said that the bitcoin theme involves human rights from an absolutely innovative point of view. Under some points of view, the protection of these rights sees its implementation thanks to some intrinsic characteristics of the network. In other circumstances, however, are precisely these characteristics of the system that undermine the effective and full enjoyment of these rights. In other circumstances, instead, the enjoyment of these rights is also hindered by the same States, which often have not been able to provide an adequate regulatory response to the growing cases of violations of human rights connected to the bitcoin network and its applications. Bitcoin phenomenon has posed a particularly and unique set of challenges for the introduction of a shared regulation amongst States. It becomes necessary to understand the root causes of the States' slowness in adapting to a phenomenon that has been evolving over the past ten years. There are five major challenges for the States when it comes to adopt a Bitcoin regulation.

Firstly, bitcoins pose a definitional challenge. Virtual currencies legal status has been until now a debated question. The reason why issues concerning virtual currency regulation have been so broadly and thoroughly examined is because of certain fundamental questions related to legal policy. Putting aside issues related to criminal use, Bitcoins not only compete with legal tender and thus represent a threat to the traditional money issuance system, but they also question the role of banks and other financial institutions in fund transfers.[253] Moreover, they combine the characteristics of currencies, commodities and payments systems. Hence, their classification on one or the other category will influence their regulatory treatment. There are cases, for instance in France,[254] in which Bitcoins are expressly excluded to receive certain legal definitions. In other countries, bitcoins may be classified in different ways, according to the regulatory authority and its own policy concern.[255] In most of other countries, where the legal status of bitcoin has yet to be determined, governments have generally opted for a wait-and-see approach: in this sense, bitcoins (or

252 EBA, *'Opinion on 'virtual currencies'*, 4 July 2014, p. 30 purchased at https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

253 M.Ishikawa, 'Designing Virtual Currency Regulation in Japan: Lessons from the Mt Gox Case', in *Journal of Financial Regulation*, vol. 3, 2017, pp. 125–131

254 Until last January 2018, when the French Minister of the Economy Bruno Le Maire created a working group with the purpose of regulating cryptocurrencies.

255 A. Sotiropoulou,, D. Guégan, 'Bitcoin and the challenges for financial regulation', in *Capital Markets Law Journal* October 2017, Vol.12, No.4, pp. 466-479

virtual currencies in general), are not regarded as a currency, but merely as a commodity that can be used for barter or exchange.[256]

Secondly, it is very difficult to monitor the use of Bitcoins. As it was already said during this work, one of the key factors, which is at the same time one of the biggest issues, is represented by the pseudoanonimity of the users. This factor, in addition to the Peer to Peer technology, make difficult to track down the identity of the users and therefore the uses for which they have transferred bitcoins.[257] The already cited cases of SilkRoad and the Deep Web are clear examples of this problem. These problematics directly introduce to the third order of issues faced by the central authorities. In light of the cross-border reach of the technology, asserting jurisdiction over a particular bitcoin transaction, or over a market participant, may prove challenging for national regulators.[258] Even if a jurisdiction may be asserted, it may anyhow be difficult for the domestic regulatory authorities to obtain information from abroad. National authorities may also find it difficult to enforce laws and regulations in a "virtual" (online) environment.[259] In this regard, taxation can be considered a relevant issue. Due the cryptocurrencies transactions' independence from any financial intermediary, it is also practically impossible to monitor where bitcoins are transferred, and consequently it is impossible to know whether in the country where the user to whom bitcoins are transferred, the latter are susceptible to tax value or not.

The decentralized nature of Bitcoins constitutes also a fourth key challenge for traditional regulatory models. The elimination of intermediary figures - such as an issuer or a payment processor - has contributed in exacerbating these regulatory issues. In such circumstances, the question then becomes how a regulatory framework for cryptocurrencies should be designed by central authorities. In this sense, the regulatory response givens so far to these challenged posed by Bitcoin and cryptocurrencies in general have varied greatly among jurisdictions. Later in this work the different approaches will be deepend. For the moment, two predominant trends can be highlighted for what concerns bitcoins' regulation: some countries have decided to ban their uses, while others have addressed some of the immediate risks. It was correctly pointed out that "*these mixed signals and divergent proposals from regulators in jurisdictions have de facto contributed to an uncertain*

256 P. De Filippi, "Bitcoin: a regulatory nightmare to a libertarian dream", in *Internet Policy Review,* March 2014, vol. 3, iss.2, p.6, available at https://policyreview.info/node/286/pdf, (accessed the 14 July 2018)

257 IMF, Staff Discussion Note, *'Virtual Currencies and Beyond: Initial Considerations'*, January 2016, retrieved at:http://www.imf.org/~/media/websites/imf/imported-full-text- , the 15/07/2018

258 Ibidem, p. 25

259 Ibidem

regulatory environment".[260] This uncertain legal status of bitcoins has tangible negative effects both for the bitcoin users and for the regulatory authorities. In order to remedy this lack of clarity, it becomes pivotal adopting some clear and targeted regulations, able to address specifically identified cryptocurrencies' risks.

Despite the willingness of the States in introducing these targeted resolutions, however, States must cope also with probably the most important issues related to the Bitcoin network: its self-enforceability and self-regulatory framework. This self-enforcement of the network is the element that strengthens the bitcoin users in claiming their independence from any kind of intervention by the central authorities. By pushing-towards this self-regulation and by implementing stateless mechanisms of adjudication, Bitcoin users became a social group able to transcend the constraints of financial institutions and the contents and boundaries of national regulation. In this sense, the need for user protection was acknowledged already in the Nakamoto paper, where it was noted that '*routing escrow mechanisms could easily be implemented to protect buyers*'.[261]In other words users can protect themselves by implementing the system in which they are operating through the adoption of 'smart contracts'.

2.11.1 Smart Contracts as the expression of the Bitcoin network self-enforcement.

When it comes to 'smart contracts', it must immediately been said that there is not an univocal definition. This should not surprise, both due to the very novel nature of this phenomena, and due to its complex technological basis. According to the simplest definition, given by Nick Szabo, '*Smart contract is an agreement whose execution is automated through a computerized transaction algorithm, which performs the terms of the contract*'.[262] In going further, it could be said that a smart contract is a piece of code which is stored on a Blockchain,[263] triggered by Blockchain transactions, and which reads and writes data in that Blockchain's database.[264]

A legitimate question arises at this point: is it possible to give to Smart contracts the meaning attributed to it by contract law?[265] This question has introduced an open debate. According to M.

260 J.W.Lim, "A facilitative Model for Cryptocurrency regulation in Singapore", in *Handbook of Digital Currencies*, Elseviert Inc., 2015 , pp. 361-381

261 S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system'

262 N. Szabo, 1994, '*Smart contracts in Essays on Smart Contracts, Commercial Controls and Security*', retrieved at http://szabo.best.vwh.net/smart.contracts.html

263 A. Savelyev, "Contract Law 2.0: «Smart» Contracts As The Beginning Of The End Of Classic Contract Law", Master Thesis, National Research University Higher School of Economics (HSE), available at https://wp.hse.ru/data/2016/12/14/1111743800/71LAW2016.pdf, p. 8 (accessed 20 July 2018)

264 G.Greenspan, *'Beware of the Impossible Smart Contract', Blockchain news*, 12 April 2016, retrieved at http://www.theblockchain.com/2016/04/12/beware-of-the-impossible-smart-contract

265 Savelyev, "Contract Law 2.0: «Smart» Contracts As The Beginning Of The End Of Classic Contract Law", Master Thesis, National Research University Higher School of Economics (HSE), available at https://wp.hse.ru/data/2016/12/14/1111743800/71LAW2016.pdf, p. 10

Raskin, smart contracts could be considered as a form of 'self-help', since a machine in order to execute the agreement doesn't need to recourse to a court.[266] On this trail also Douglas Brandon has said that self-help could be understood as the "*legally permissible conduct that individuals undertake absent the compulsion of law and without the assistance of a government official in efforts to prevent or remedy a civil wrong*".[267]

Other scholars, instead, deviate from this view, since appears to be too simplistic. [268] This other currency believes that the first kind of approach deprives Smart contracts of the deeper analysis within the framework of contract law they should deserve. Moreover, this new currency of thought believes that "*there are several factors which point to affirm that Smart contracts can be regarded as a legally-binding agreement*".[269] First of all, Smart contracts can be used to discipline the circulation of certain digital assets, aiming to govern economic relations between the parties, qualifying hence a "legal effect" within the contract. Secondly, although Smart contract's performance is automated, it still requires the presence of the will of the party in order to become effective.[270] This will manifest itself in the moment an individual decides to use an electronic agent for the conclusion of certain agreements and agrees to be bound by their actions.[271] The mere fact that the contract is concluded by electronic means does not mean that it is not a contract.

In order to understand the functioning of smart contracts, it is necessary to outline their features. On the basis of what has been said until now about smart contracts, it is possible to enlist the following features:

1) *Solely electronic nature*: while classic contracts may exist in various forms, for instance in oral form or in writing, smart contracts may exist only in electronic form. It is also driven by the specifics of the subject matter of smart contracts. A smart contract may relate to certain digital assets (i.e., cryptocurrency) or digital manifestations of offline assets, title to which is registered in Blockchain.[272]

266 M.Raskin, "The Law of Smart Contracts", in *Georgetown Law Technology Review,* vol. 304, 2017, p. 333

267 I B Douglas et al., " Self-Help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society", in *Vanerbilt La. Rev,* 1984, vol. 37, pp.845- 850.

268 A. Savelyev, "*Contract Law 2.0: «Smart» Contracts As The Beginning Of The End Of Classic Contract Law*", 2016, National Research University Higher School of Economics (HSE) p. 10, available from https://wp.hse.ru/data/2016/12/14/1111743800/71LAW2016.pdf

269 Ibidem.

270 A. Savelyev, "*Contract Law 2.0: «Smart» Contracts As The Beginning Of The End Of Classic Contract Law*", 2016, National Research University Higher School of Economics (HSE) p. 11, available from https://wp.hse.ru/data/2016/12/14/1111743800/71LAW2016.pdf

271 Ibidem

272 A. Savelyev, "*Contract Law 2.0: «Smart» Contracts As The Beginning Of The End Of Classic Contract Law*", 2016, National Research University Higher School of Economics (HSE) p. 12, available from https://wp.hse.ru/data/2016/12/14/1111743800/71LAW2016.pdf

2) *Software-implementation*: if in the real world the law is represented by Civil and Criminal Codes, in smart contracts' world computer codes define contractual terms. Thus, "*contractual terms are manifested in a computer code, what is not generally prohibited based on the "freedom of contract" principle"*.[273]

3) *Increased certainty*: since smart contract are having software codes in their core, their terms are expressed in one of computer languages, which have a strictly defined semantics and which don't allow discretion in their interpretation by machine.[274] An higher precision in programming languages is hence able to mitigate possible issues associated with misinterpretations of contractual terms by the parties. Although it is possible to find ambiguities within programming languages, they are much lower than in the real world because there are constituted by simple terms easily recognizable by a computer.

4) *Self-enforceability*. Once a Smart contract is concluded, its execution doesn't depend anymore on the will of its parties or third parties.[275] The tasks of verifying the respect of all the conditions, transferring assets from a wallet to another and registering such transfers in the Blockchain database are all demanded to computers.

5) *Self-sufficiency*: it is closely related to the previous feature, but it characterized by a different emphasis.[276] Smart contracts don't need any legal institutions in order to exist and to be valid. Self-sufficiency becomes especially important in cross-border transactions, as it allows not to depend on differences in languages, national laws and their interpretation.

The abovementioned features allow to smart contracts as a '*a software code (or part of it), implemented on the Blockchain platform, which guarantees the self-implementing and autonomous nature of its terms, triggered by conditions defined in advance and applied to Blockchain '*.[277]

Despite their innovativeness, smart contracts still create lots of concerns and challenges when it comes to apply classic concepts of contract law to them. Moreover, such challenges have universal nature, going to the core of contract law provisions, which are more or less the same regardless of the jurisdiction. One of the main problems lies in the fact that smart contracts were created to be

273 Ibidem.

274 A.Savelyev, "*Contract Law 2.0: «Smart» Contracts As The Beginning Of The End Of Classic Contract Law*", 2016, National Research University Higher School of Economics (HSE) p. 13

275 Ibidem, p. 15

276 Ibidem.

277 A.Savelyev, "*Contract Law 2.0: «Smart» Contracts As The Beginning Of The End Of Classic Contract Law*", 2016, National Research University Higher School of Economics (HSE)

developed in a technical universe, "parallel" to legal realm. Furthermore, the solely technical code enforcement of smart contracts' provisions leads to further issues. Firstly, it could be argued that smart contracts don't create legal obligations. This lack of legal obligations, in classic legal sense, leads to conclusion that all the legal regimes associated to obligations – from the modes of performance to the consequences of non-performance - are not applicable.[278]

Secondly, both vitiated consents or intents do not have any impact on Smart contract's validity. It is completely irrelevant for its performance if a smart contract was realized for mistake or as a result of fraudulent misrepresentation, coercion or threats. Smart contracts don't allow to ensure protection of weak parties. The whole layer of legal provisions relating to consumer law and unfair contract terms is non-applicable to smart contract. This egalitarian nature applies not only towards the subjects involved within the contract, but also to the objects of the contracts themselves. smart contracts are treating legal and illegal subject matter in the same way. What it matters is only the possibility to implement such subject matter in a code.[279] These issues have contributed to the reason why governments have always looked with a critical eye and mistrust towards smart contracts.

Nevertheless, it must be noted and appreciated that Bitcoin didn't create only a network and a cryptocurrency, but also a new form of expression of parties' autonomy. Pietro Ortolani has said that "*code becomes a new language of contract: the parties, by devising these escrow scripts, aim at achieving a result, resembling what it could be -latu sensu – qualified as an arbitration agreement*".[280] Bitcoin and smart contracts, thus, open the field for a new evolution of contract-making, where codes replace traditional languages. The great introduction of smart contracts is that they don't need a legal system to exist. They may operate without any overarching legal framework, representing a new technological alternative to legal systems.[281]

2.12 Final Considerations

In conclusion to this second chapter, it is possible to operate the following considerations. It is undeniable that Bitcoin technology features have direct points of contact with the human rights. In some situations, these interactions can contribute or are actually contributing in enhancing the

278 Ibidem, p. 18

279 Ibidem, p. 19

280 P. Ortolani, The Three Challenges of Stateless Justice, in *Journal of International Dispute Settlement*, 2016, vol. 7, pp- 596.627, p. 605

281 A.Savelyev, "*Contract Law 2.0: «Smart» Contracts As The Beginning Of The End Of Classic Contract Law*", 2016, National Research University Higher School of Economics (HSE), p. 21

enjoyment of users' human rights. A clear example of that is the application of cryptography as a form of protection of the right to privacy. In this sense, it has to be appreciated the willingness of European Union in following these social and technological developments, aiming to provide a prompt legal response to all the new possible violations of the right to privacy. On the other hand, it must be noted the absolute absence, in particular within the GDPR, of any possible legal reference, suitable for taking into consideration the possible uses of the blockchain and its potential dangers toward individuals' privacy. More specifically, despite the focus on defining pseudonymisation has to be appreciated, no legal warranty is given to the individuals whom the pseudonymised can be hacked. With particular focus to the Bitcoin network, blockchain technology affects the peers' privacy in several ways. The lacks of legal coverages can be as well applied also to the issues faced in exercising the right of property. Bitcoin system of property protection rests on the theoretical perfection of the private key/public key mechanism, assuming that users are perfectly able to fully exercise their property on and to implement the security of the whole network. On the other hand, conversely, both from the Bitcoin network, but more and foremost by the States, a concrete legal solution, able to cope with the issues associated in the enjoyment of the right to property is still missing. Therefore, many questions still do not find accurate answers. Can bitcoins fall within the notion of property? What happens if a bitcoin *user* (both an *investor* or a *miner*) loose or is robbed of his bitcoins? Can he/she apply to a national court? This kind of questions are also valid for what concerns the right to work. Are the people who are actively working in the Bitcoin network sufficiently protected by the European and national laws? What kind of responsibilities the employers and the employees have?

All these questions lead to a specific direction: Bitcoin phenomenon is no longer a simple mania that was limited to a few enthusiasts and experts in the computer industry. It is a phenomenon that is involving more and more people and that, inevitably, will require more and more attention from the states. The current regulatory framework in Europe provides interesting insights from which states should start in order to improve the legal situation of the individuals concerned.

CHAPTER III
- STATES APPROACHES TO BITCOIN ISSUES -

Introduction

After having previously pointed out what are the major issues faced by the users and what are the difficulties the States are encountering in introducing regulation about the Bitcoin this final chapter will focus on the approaches European States are adopting toward Bitcoin issues. The purposes of this chapter will be to evaluate if the different approaches adopted by the European States are

concretely able to cope with the issues faced by the users and, foremost, if they are complying with the obligations descending from the European covenants. In order to achieve these goals, it will be carried out a comparative analysis between the different trends of some European countries, based on a list created by J.D. Hansen.[282] This list, updated on an ongoing basis, includes in alphabetical order all the Countries of the World, and how they are dealing with the cryptocurrencies. Before proceeding to this comparison, will be identified the main areas of intervention which States must consider before adopting a regulation. The identification of these areas becomes necessary in order to understand in which direction the States' attentions should be addressed, so as to be able to give an exhaustive answer to the problems associated with the Bitcoin network.

After having carried out a human-rights related analysis over the different European States trends, the chapter will conclude by furnishing some recommendations according to which a cooperation between States and users' community could be achieved. The aim of these recommendations will be to give a new, possible approach States might adopt in order to both coping with the Bitcoin and the block-chain technology human rights violations as well as being able to comply with their obligations in order to prevent these violations.

3.1. The possible areas of intervention that should be subject to regulation.

In having determined what are the major issues associated to cryptocurrencies' regulations, another question rise up: which areas should be taken in exam for a specific regulation by States? By combining the issues faced both by governments (in adopting a targeted regulation) and by the users (in exercising their rights), it is possible to identify three possible areas of intervention: Bitcoin system, Bitcoin uses and Bitcoin users. These three areas, despite are undoubtedly intertwined, should require specific attentions.

Bitcoin system. A possible regulation should consider the whole Bitcoin scheme itself, which means the Bitcoin protocol and the rules governing the operation of the system to which all participants in the network decide to adhere.[283] Nevertheless, on the basis of the objective difficulties afore described, a regulation of the Bitcoin network may prove extremely difficult. The absence of a central authority, able to administer and control the system, as well as be subject to regulations, makes impossible to set up a regulation which could be applied. Moreover, those who substitute

282 J.D.Hansen, *Digital Currencies: International Actions and Regulations*, available at https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html#austria, accessed the 21st July 2018.

283 A. Sotiropoulou,, D. Guégan, 'Bitcoin and the challenges for financial regulation', in *Capital Markets Law Journal* October 2017, Vol.12, No.4, p. 472

the central authorities are miners and developers, whom are indeed numerous, but their identities are unknown. Regulatory authorities within the network could only play the role of collector of complaints of the users and issue communication and warning on the problems that arise. In this sense, they should set up some information platforms where the users can provide information and be informed about dysfunctions of the network.

Bitcoin uses. A second area of regulation should focus on the uses of bitcoin. More specifically, these regulations should target the illegal uses made with bitcoins. On one hand, the 'non-face-to-face' customers relationship characteristic of Bitcoin network enhances the enjoyment of users' privacy, through an almost-complete pseudoanonimity; on the other hand, it contributes in raising concerns about the sources of fund or the purposes to which funding for bitcoins are put. The real challenge for States therefore becomes to find a right balance between guaranteeing the right to privacy of the users, but at the same time being able to limit it when it is made up of illegal uses. If bitcoins are used for making payments or for exchanges for fiat currencies it is evident that they don't serve for an illegal purpose. On the contrary, when they are used for money laundering or for financing terrorism, it comes clear that possible regulations should focus particularly towards these illegal uses. While in the traditional payment systems, the banks and conventional providers of money or money are the pivotal subjects who ensure that Anti Money Laundering (AML) and Combating Financing Terrorism (CFT) regulations are observed, in the Bitcoin network these subjects are absent.[284] About this, the Financial Action Task Force (FATF), in its 'Guidance for a risk-based approach towards virtual currencies',[285] has also stated that '*virtual currency's global reach increases its potential AML/CFT risks*'.[286] In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. By issuing a guidance on the application of the international AML/CTF standards towards virtual currencies, FATF has identified the intermediaries as possible subjects of the obligations.[287] Imposing AML/CTF regulations only on exchanges may not be sufficient, and therefore some regulators have proposed to extend these obligations also to wallet service providers that operate within the Bitcoin system. Nevertheless, it has to be stressed that the application of the AML/CTF regulations to the Bitcoin sphere won't

284 A. Sotiropoulou & D. Guégan, Bitcoin and the Challenges for financial regulation, in *Capital Markets Law Journal*, Vol. 12, n 4, pp.466-479

285 FATF, GUIDANCE FOR A RISK-BASED APPROACH VIRTUAL CURRENCIES. retrieved at http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf, 20 July 2018

286 Ibid, p. 32

287 A. Sotiropoulou & D. Guégan, Bitcoin and the Challenges for financial regulation, in *Capital Markets Law Journal*, Vol. 12, n 4, pp.466-479

be totally effective, since a significant part of the transactions could be conducted without the involvement of exchangers or wallet service providers.

European regulators have started to moving in this direction, by adapting the existing AML/CFT regulations to cryptocurrencies' schemes, in particular to virtual currencies/fiat currencies exchangers as well as to custodian wallet providers. The recent EU Directive 2018/843 aims to address the anonymity of the financial technology, by implementing rules for cryptocurrency exchanges, platforms and wallet providers. Under the measures, such entities must be registered with authorities and will to have to apply due diligence procedures, including customer verification. The explicit recognition of these professional roles has two important consequences: first, it represents the will of the European legislators to interface with this new cultural and technological paradigm, and therefore to introduce specific rules in order to provide adequate legal discipline. Secondly, it allows these new professions to be almost completely protected by the rules already present in the juridical law that protect and regulate professionals who offer similar services.

Bitcoin users. A third order of regulations should take into account the users of Bitcoin. In particular, according to the definition afore considered in paragraph 2.4, the users taken into consideration should be miners and investors. The adoption of a regulation on the protection of miners encounters some practical issues, already indicated in paragraph 2.6, which make it objectively impossible for legislators to apply the existing regulations on the right to work to this particular professional figure. On the other hand, the protection of investors is undoubtedly much easier to achieve. Bitcoin investors should be aware of the risks associated to the use of bitcoins: in particular, they should be aware of the irreversibility of transactions and the volatility of bitcoins' value.[288] These risks are inherent to operations within the Bitcoin network which, as we have seen within this paragraph, is impossible to submit to specific regulation. With a particular focus on the irreversibility of transactions, this risk may have critical consequences over users' right to property.

The loss or theft bitcoins (or the private key) directly affects their peaceful enjoyment of their possession of bitcoins. Once stolen bitcoins are transferred to another wallet, and the transaction is transcribed within the block-chain ledger, it is impossible to have the right to property restored. This risk derives from an intrinsic characteristic of the network, it could not be modified by any regulation. Users' protection may be achieved through adoption of disclosures, able to create

288 A. Sotiropoulou & D. Guégan, Bitcoin and the Challenges for financial regulation, in *Capital Markets Law Journal*, Vol. 12, n 4, p. 474

awareness, among possible future investors, about the risks associated to Bitcoin networks and bitcoin operations. These disclosures could contribute in reducing – or even eliminating- the dangers within the network. For what concerns the volatility of bitcoins' value, this is a factor which depends on the law of 'supply and demand' on the market and on the consequent diffusion and acceptance of bitcoins as a means of payment. The more bitcoins will be accepted as an alternative form of payment, the more their value will increase. Therefore, it will be necessary a financial regulation, able to cope with the issues of systemic risks and financial stability.

3.2 The possible States' approaches towards the cryptocurrencies. Are they human rights oriented?

Bearing in mind both the difficulties encountered by the States in introducing regulations, the human rights' violations faced by users and workers and the possible areas of interventions, it is possible to proceed in identifying the approaches European States are having towards the Bitcoin network and blockchain technology and to evaluate whether they are human rights oriented or if they need to be implemented. As it was stated in the introduction of this chapter, this analysis will he carried out by comparing the different trends amongst some of the Member States of the European Union. All the chosen States have signed and ratified both the ECHR and the EU Charter of Fundamental Rights and they are therefore subject to the obligations descending from these Conventions. Moreover, in quality of Member States of the European Union, these states must comply also with the duties and obligations of the GDPR. They should also embrace the new introduction proposed by recent Directive 2018/843 on AML/CTF.

In carrying out this comparative analysis of the different orientations of States, it was immediately possible to notice a change in tendency from parts of many European states in recent years. Apart from a few small cases of countries that remained anchored to conservative positions or aimed at minimizing the risks deriving from "naive" approaches to technology, many States have understood that the Bitcoin phenomenon is constantly evolving and have therefore decided to change their mentality and their positions towards this technology trying to adapt and introduce regulations that follow this evolution. This has translated into different ways of approaching to the different problems that this cultural paradigm has introduced. It was therefore possible to identify four different types of approach, updated at the end of June 2018, which reflect different cultural and regulatory orientations with respect to the phenomenon of cryptocurrencies. The following table will list all the States considered in this analysis, clustered in the respective approach group.

The States in green are those who are willing to adopt, o have already adopted, specific regulations over Bitcoins.

Monitoring	*Recommendations*	*Guidances*	*Regulations*
			Austria
			Belgium
			Croatia
	Denmark		
	France		
		Germany	
	Greece		
	Hungary		
Ireland			
	Italy		
	Netherlands		
	Portugal		
		Poland	
			Slovenia
			Spain
		Sweden	

Monitoring. A first approach, very residual, approach is the one that just takes into account the 'monitoring' of the Bitcoin phenomenon. According to this type of approach, a State authority -

usually an institution entitled to supervise financial institutions - although it is aware of the existence of Bitcoin network and bitcoins operations, has issued a statement according to which there is the "intention" of dealing with this phenomenon in the future. [289] This type of approach is now a minority, since it has only been adopted in Ireland. From a human rights perspective, this approach has several negative consequences. The absence of concrete actions by the State damages, at the same time, both the people who have decided to invest economically in this currency, and those who have undertaken professional careers in the area of Bitcoin. The lack of State intervention on the uses of Bitcoin, as well as the unwillingness in introducing at least warnings about the risks associated to the block-chain technology and bitcoins' operations, lead to the proliferation of these risks, as well as an increase of the risk of the violations of the human rights of the people involved in the Network. A State who chooses this approach is directly refusing to comply with its obligations to respect, protect and fulfil the rights of the users and the workers who have chosen to believe in this technology. Although this approach is limited to the Irish case alone, it still raises concerns about the protection of the right-holders of the Bitcoin network.

Recommendation. A second, more widespread, type of approach among Member States is the one which sees the adoption of specific recommendations by States. This type of approach is characterized not only by the express recognition of bitcoins' existence by a State authority, but also by the issue of specific recommendations, aiming to increase the knowledge among the citizens who want to approach the Bitcoin world.[290] These recommendations can be divided into two main groups: on the one hand, we have recommendations that aim at warning about the risks associated with Bitcoin technology and transactions. It is possible to find these warnings in several European countries, such as Belgium, Denmark, France, Greece, Hungary, Italy, Netherlands and Portugal. On the other hand, there are recommendations in which a State authority has issued statements related to the potentialities of cryptocurrencies.[291] This approach is used only in Croatia, where the National Bank of Croatia has allowed the use of bitcoins, praising the potential of bitcoin transactions.[292]

289 J.Lansky, 'Possible State Approaches to Cryptocurrencies', in *Journal of Systems Integration*, vol. 1, 2018, pp. 19-31.

290 J.Lansky, 'Possible State Approaches to Cryptocurrencies', in *Journal of Systems Integration*, vol. 1, 2018, pp. 19-31.

291 Moreover, these statements have also recognized that cryptocurrencies do not retain personal data of their owners, preventing, in this sense, any possible risk of misusing these personal data, in accordance with the principles of the GDPR.

292 '*Croatia has allowed the Use of Bitcoins*', 16 December 2013, retrieved at https://coinspot.io/europe_and_russia/xorvatiya-razreshila-ispolzovanie-bitkoina/, (accessed the 23 July 2018)

Based on what has been said about areas of States' intervention, there is no doubt that this second set of regulations has signed an important first step towards the integration of the Bitcoin phenomenon within the national legal frameworks. By creating awareness about the risks, States are aiming at reducing the potential issues associated to Bitcoin technology. In this sense, the prevention of possible violations of the human rights of new (possible) Bitcoins' users aiming, at the same time, to comply with the states' obligation to protect the rights, must be appreciated and encouraged. However, the only human right that finds a kind of protection in this sense is the right to property. Through their recommendations, States takes into account only the risks associated to the deprivation of property. Obviously, the extent of this prevention of deprivation changes according to the definition given to property in each country. Therefore, the effective protection of the right to property changes according to how risk recommendations can be reconciled with the definition of ownership in individual legal systems. It seems clear that this approach presents however some practical issues. Despite its clear aim is to prevent the proliferation of the risks, this approach has the huge limit that doesn't propose concrete solutions in order to solve them. Moreover, both right to privacy and right to work are not minimally covered by the recommendations made by the States. This 'non-consideration' contributes to increasing the already existing problems in the enjoyment of these rights. For what concerns the right to property, not taking into consideration the risks associated with the possible negative uses of the right to privacy that derives from the pseudoanonimity of the users leads to two negative consequences: on the one hand, it puts the safety of users at serious risk, as well as encourages the risk that bitcoins are used to purposes of money laundering and / or terrorist financing. On the other hand, the absence of guidelines precludes any possible intervention by the States in limiting the exercise of this right for security reasons. For what concern the right to work, instead, by non-taking into account working figures such as the exchangers and consultants, States are not only not respecting their right to work, but they are not even providing adequate protections deriving from the various rules on labour law, such as the prohibition of forced work, exploitation and non-discrimination.

Guidance. Moving from this second approach, some European States decided to make a step further. In this sense, hence, States have accompanied the warnings on the bitcoins' risks with specific guidances in order to govern the method of using cryptocurrencies. These guidelines refer in particular to the kind of value attributed to bitcoins, especially for VAT purposes. In this sense, therefore, we can distinguish different approaches between states. There are states, among which it should be mentioned Germany and Sweden, which consider bitcoins as a kind of assets, whose

gains derived from their ownership or from their sale makes bitcoins subject to national tax legislation applicable to assets. In other countries, instead, cryptocurrencies are considered as goods and ought to be subject to VAT.[293] A particular situation could be found in Spain, where bitcoins are subject to gambling tax and in Poland and Slovenia, where mining activity is subject to VAT.

At the European level it must be remembered the adoption of the recent AML/CTF directive, which has introduced two important innovations. Firstly, the Directive introduces specific discipline regarding exchangers and consultants.[294] The second, equally important, innovation resides in the obligations imposed on these two new categories of subjects regarding the monitoring of the origin of the sums invested and exchanged in bitcoins. From the combined reading of Articles 9 and 12 of the Directive it is evident the will to discourage the illicit uses associated to the bitcoins but, above all, to adopt an innovative approach that "*allows to obtain information which allow to associate virtual currencies addresses to the identity of the owner of virtual currency*."[295] Moreover, Article 12 also adds that "*business relationships or transactions involving high-risk third countries should be limited when significant weaknesses in the AML / CFT regime of the third-country concerned are identified*".[296]

With reference to this third approach, it is possible to notice that there are two different tendencies. A first is the attempt by States to assign a defined legal value to bitcoins, namely if they are assets subject to property or not. In determining what value should be attributed to bitcoins, it is evident each approach is based on the national regulation regarding the definitions of property and the key elements associated. All these different approaches have shown the willingness of the Member States to change their mindsets about bitcoins and to try to furnish a legal answer to what concerns bitcoins' ownership. Nevertheless, despite these new States' approaches must be favourably acknowledged, are still missing judicial remedies for the victims of bitcoin theft. This therefore precludes full satisfaction of the right to property. Above all, in those states in which Bitcoins have been recognized as property subject to property rights, the continuing absence of legal remedies constitutes a violation of the same States with regard to their obligations to protect and fulfil.

On the other hand, a positive trend has to be remarked for what concerns the adoption of the Directive 843/2018 on Anti money Laundering or Terrorist Financing. Undoubtedly, the great limit

293 A clear example of this is France, where Bitcoins are considered as movable properties and are subjected to the correspondent VAT taxation.

294 EU DIRECTIVE 843/2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, article 8, available at http://data.consilium.europa.eu/doc/document/ST-15605-2016-INIT/en/pdf

295 Ibid., Article 9. available at http://data.consilium.europa.eu/doc/document/ST-15605-2016-INIT/en/pdf

296 Ibid., Artcile 12.available at http://data.consilium.europa.eu/doc/document/ST-15605-2016-INIT/en/pdf

of such Directive is that it considers only exchanges of fiat currencies and bitcoins operated through exchangers. Nothing has been said about the exchanges between privates as sources of money laundering of terrorism financing. The lack of regulation about these exchanges raises, once again, the question on how the Governments should, instead, take into account the cross-border reach of the Bitcoin technology, and how to control the users on a global scale. Nevertheless, the important innovations previously mentioned have very important legal consequences for the implementation and protection of human rights that are the subject of this work. The close collaboration between the States, the Financial Information Units (FIU) and these new professional figures guarantees a full legal recognition of the latter within national laws. This constitutes an important step forward in terms of guarantees of human rights, as it allows the guarantees arising from the articles on the right to work both in the ECHR and in the EU Charter to be applied to these categories. In particular, the guarantees deriving from Article 4 and 14 of the ECHR find their fulfilment through this recognition. Moreover, the duties imposed to exchangers and consultants have direct consequences on the right to privacy of the users. In particular, exchangers play a pivotal role through their activities of monitoring the uses of virtual currencies, allowing the competent States' authorities to receive all the relevant information able to limit the uses of bitcoins for money laundering or terrorist financing purposes. By associating virtual currencies addresses to the identities of the respective owners of the virtual currencies, the Directive opens up to the possibility of interfering within the private sphere of individuals. On the basis of what has been said in Paragraph 2.8.1, it is not possible to detect a violation of the right to property in this sense, since the interference from the State is justified by its intrinsic legitimacy, and it aims to reach a legitimate interest which is perfectly foreseeable by the same users. The same Directive 843/2018 is very clear on this point, when at Article 41 [297] and 42 explicitly mentions that it is State's duty to clearly define within its legal framework what is considered 'legitimate interest', *'both as a general concept and as a criterion for accessing beneficial ownership information in their national law."*[298] Indeed, this third approach presents several very interesting features. In recurring to it,

297 EU DIRECTIVE 843/2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Article 41: "*Access to information and the definition of legitimate interest should be governed by the law of the Member State where the trustee of a trust or person holding an equivalent position in a similar legal arrangement is established or resides. Where the trustee of the trust or person holding equivalent position in similar legal arrangement is not established or does not reside in any Member State, access to information and the definition of legitimate interest should be governed by the law of the Member State where the beneficial ownership information of the trust or similar legal arrangement is registered in accordance with the provisions of this Directive*."

298 EU DIRECTIVE 843/2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Article 42: "*Member States should define legitimate interest, both as a general concept and as a criterion for accessing beneficial ownership information in their national law. In particular, those definitions should not restrict the concept of legitimate interest to cases of pending administrative or legal proceedings and should enable to take into account the preventive work in the field of anti-money laundering, counter terrorist financing and associate predicate offences undertaken by non-governmental organisations and investigative journalists, where appropriate. Once the interconnection of Member States' beneficial ownership registers is in place, both national and cross-border access to each Member State's register should be granted based on the definition of legitimate interest of the Member State where the information relating to the beneficial ownership of the trust or similar legal arrangement has been*

States aim to discipline both the uses and the users and exchangers of bitcoins. They also are having a practical look toward the value added taxes which can be imposed to the ownership of bitcoins and to the working activities connected to the network. The sooner this directive will be implemented within the Member States, the better the protection of these new working figures will grow and the controls towards the illegal uses of bitcoins will be implemented.

Regulation. A fourth approach is focused on the introduction of regulatory frameworks. In some cases, Austria, Croatia, Slovenia and Spain, these regulations aim to a progressive integration of bitcoins as a currency equivalent to fiat currencies; in other countries, conversely, States aim to more restrictive policies focused on banning or refusing the use and adoption of bitcoins. In Belgium, for instance, the Minister of Justice has affirmed that, "*since cryptocurrencies are used by terrorists, criminals, and drug dealers, it is necessary to adopt a regulation that aims to confiscate all cryptocurrencies in circulation or, in the most extreme cases, to proceed to a ban of these currencies*".[299] Such a restrictive kind of approach has, inevitably, negative consequences over the human rights of the users. Firstly, in stating that since there are illegal uses of bitcoins, they need to be all confiscated, a State is clearly manifesting its inadequacy in distinguishing those who are operating illegally from those who are actually investing or working in accordance to the law. This conduces to a dangerous generalization which entails the rights of those individuals who are investing and working in Bitcoin, without any legal basis. The Belgian (possible) regulation, furthermore, doesn't take into account the basic features of the Bitcoin technology: its cross-border reach diffusion and the anonymity of the users. On which basis this confiscation could be realized? How is it possible to associate a Bitcoin wallet to a terrorist, a criminal or a drug dealer which is operating in Belgium? This approach doesn't seem to give the proper responses. In such approach, it the foreseeability necessary to operate an interference by the State can't be perceived from the addressees of these measures. This implies that the limitation of the rights – in particular of the right to property and the right to work - is happening on a purely arbitrary basis. For what concerns the right to work, this approach leads to an open discrimination towards all those honest workers,

registered in accordance with the provisions of this Directive, by virtue of a decision taken by the relevant authorities of that Member State. In relation to Member States' beneficial ownership registers, it should also be possible for Member States to establish appeal mechanisms against decisions which grant or deny access to beneficial ownership information. With a view to ensuring coherent and efficient registration and information exchange, Member States should ensure that their authority in charge of the register set up for the beneficial ownership information of trusts and similar legal arrangements cooperates with its counterparts in other Member States, sharing information concerning trusts and similar legal arrangements governed by the law of one Member State and administered in another Member State."

299 N. Lyon, ***B****elgium to Restrict All Transactions with Bitcoin*, 17th April 2017, retrieved at https://coinidol.com/belgium-to-restrict-all-transactions-with-bitcoin, the 27 July 2018.

who invested their savings for the start of their legal activities. It seems evident that, if the willingness if to fight the illegal uses of bitcoins, associated to money laundering of financing terrorism, this kind of regulation is not the answer. They are not able neither to give an adequate solution to the illegal uses, nor to comply with the States' obligations of respecting human rights of the honest investors, exchangers and consultants.

By contrast, Austria's finance ministry has recently proposed to look at the trading rules for gold and derivatives as an inspiration in order to draw up regulations on cryptocurrencies for the nation and for the European Union.[300] The aim of pledging to these tighten rules is to fight money laundering and to bring trading platforms under the kind of oversight that already exists for financial instruments. This kind of regulation incorporates the same aims of the recent AML directive, but it goes further. It has not only the great merit of relying on defined legal bases within the Austrian legal system, but also of providing a precise nomenclature of ownership applicable to bitcoins. The Austria proposal is able to give an adequate legal protection not only to the users of bitcoins, but also to exchangers, which have the duty to report bitcoins' trades exceeding 10,000 euros to the financial intelligence units, similar to companies that handle large amounts of cash, gold or jewellery. In this way, their work finds specific rules and protections within the Austrian legal framework, and it doesn't risk to be jeopardized by normative lacks.

Following this trend, the Spanish Congress has made a huge step forward, by unanimously supporting a draft legislation which aim at introducing a regulation on blockchain technology and cryptocurrencies received.[301] The Spanish proposal aims to introduce the Bitcoin and block-chain technologies to the Spanish market through "controlled testing environments," commonly referred to as "*regulatory sandboxes*".[302] The draft also proposed the government to cooperate with the National Securities Market Commission and the Bank of Spain to coordinate a common regulatory position regarding cryptocurrency in the broader European context. The Congress has agreed to promote blockchain technology as an efficient and decentralized system for payments and transfers, emphasizing above all the need to strengthen fintech start-ups. Equally necessary will be the "proportionate mechanisms" to ensure that all entities implementing the new technology comply with their tax obligations. The document also highlights potential pitfalls associated with "high

300 B. Groendahl, '*Austria Eyes Bitcoin Rules Based on Gold, Derivatives'*, Bloomber.com, 23 February 2018, retrieved at https://www.bloomberg.com/news/articles/2018-02-23/austria-seeks-bitcoin-rules-based-on-gold-derivatives-controls, the 27 July 2018.

301 Bitcoin Prices Rise; Spain Supports Crypto Regulation, Cryptocurrency News, 1st June 2018, retrieved at https://www.investing.com/news/cryptocurrency-news/bitcoin-prices-rise-spain-supports-crypto-regulation-1474579, the 27 July 2018

302 Ibidem.

risk" financial assets, deeming that "adequate disclosure of information" is fundamental in order to protect investors. In this sense, the initiative proposes that the government cooperate with the National Commission for the Securities Market (CNMV) and with the Bank of Spain to agree a common normative position regarding cryptocurrencies.[303] The Spanish 'experiment' could enhance new forms of understanding of Bitcoin and block-chain technologies. This could lead to positive insights for the implementation of the protection of the rights of the users and workers involved – by adapting their situation within the Spanish existing legal framework. At the same time, this approach may facilitate the adoption of some of the basic features of the Bitcoin network – such as its self-enforceability – in order to implement the protection of human rights also outside the network.

In trying to adapt the intrinsic characteristics of the network to the existing legal frameworks, it has to be noted and appreciated the countertrend approach that has been taken into consideration in Croatia and Slovenia. In both cases, the impetus to adopt regulation did not come from above, from the state authorities, but from the same communities of users and experts in the sector. Croatia has always proved to be among the most advanced states regarding the approach and comparison of bitcoins and other cryptocurrencies. In 2013, during a dialogue on digital currencies, the Croatian National Bank declared that bitcoin was not illegal in the country.[304] More recently, in 2017, the Croatian National Bank declared that cryptocurrencies were neither the authorized cost technique nor that they came under current legislation in Croatia.[305] In February 2018, businesses and fans in Croatia have united their efforts to assist authorities take knowledgeable choices in regards to the cryptocurrency sector.[306] This has led to the creation of a self-regulatory blockchain organization called the UBIK. The latter is an autonomous body that comprises primarily of blockchain developers, businessmen and crypto enthusiasts from Croatia and other surrounding regions. The goal of this organization is to provide the masses with knowledge pertaining to the blockchain and crypto domain, so that casual investors can also take part in the crypto boom that is being witnessed

303 M. Huillet, "Spagna: proposta a favore di criptovalute e blockchain ottiene l'unanimità del Congresso", Cointelegraph.com, 31st May 2018, retrieved at https://it.cointelegraph.com/news/spain-innovation-aimed-crypto-regulation-wins-cross-party-support-in-congress, the 27 JUly 2018.

304 "Croatian central bank establishes that Bitcoin is legal in Croatia", Reddit.com, 10 December 2013, https://www.reddit.com/r/Bitcoin/comments/1sjgby/croatian_central_bank_establishes_that_bitcoin_is/, accessed the 28 july 2018

305 "CNB: investendo in bitcoin, si assume completamente il rischio", Monitor.hr, 24 September 2017, available at http://www.monitor.hr/hnb-ulaganjem-u-bitcoin-u-cijelosti-preuzimate-rizik/, (accessed the 28 july 2018)

306 *Steps towards Self-Regulation in Croatia and Slovenia*, Bitcoins.net, 18 February 2018 retrieved at https://www.bitscoins.net/steps-towards-self-regulation-in-croatia-and-slovenia/, 28 July 2018

worldwide.[307] UBIK aims to help national financial authorities with a wide array of legal and financial matters so that a regulatory framework can be developed in the coming future.[308] At the same time, in Slovenia, Government officers and blockchain firms promised to work collectively to "educate the public on the benefits and the opportunities that the innovative technology brings". They met to arrange an open dialogue between authorities and entrepreneurs, essential to make clear and deal with the challenges.[309] Both these initiatives introduce a new, possible path towards the adoption of a shared regulation both by the Governments and by the users. For the first time, users are not in an antagonistic position to their governments. Instead, they want to collaborate actively in order to give an "internal" point of view to the network. This cooperation can lead to the adoption of a regulation which is not imposed from outside, but which is the result of a shared approach between the right-holders and the duty-bearers. In this sense, from a Human Right Based Approach perspective, these approaches are those who can better enhance the protection of the human rights involved in the Bitcoin network and in the block-chain technology.

3.3. The possible outcomes resulting from these approaches. Is a regulation toward bitcoin perceived as necessary?

Determining the future role of the cryptocurrencies appears hence a very hard task. There are different factors that can affect a possible regulation of Bitcoins. A first factor, which was just analysed in the previous paragraph, will be the possible States' reactions in the near future towards this phenomenon. Some states, the most up-to-date, will continue to strive for the introduction of regulation in order to allow a role for bitcoins as part of the 'monetary ecosystem'.[310] Other states, more conservatives, will continue in overseeing the market or will shut down the virtual currencies-related business, due their possible illegality. A secondary, but still crucial factor will be the social acceptance of virtual currencies by merchants and common users as a valid alternative form of payment. In this sense, the possible outcomes can be two: on the one hand, the growing acceptance of the society to use bitcoins as an alternative means of payment; on the other, the total lack of acceptance of this phenomenon, which could lead to its inevitable disappearance. These

307 S. Jagati, '*Croatia Launches Self-Regulating Blockchain Organization*', Cryptoslate.com, 21st February 2018, available at https://cryptoslate.com/croatia-launches-self-regulating-blockchain-organization/, the 28 July 2018

308 Members of UBIK had been convening with Croatian Tax Officials since Feb. 9 to work on a legal framework that would look at the issue of cryptocurrencies being taxed as "capital gains" as well for regulating ICOs (Initial Coin Offerings). For further information, see L. Krancir, "UBIK ha iniziato a lavorare attivamente nell'area della blockchain e della cryptovalute", Crobitcoin.com, 15 february 2018, available at. https://crobitcoin.com/ubik-aktivno-krenuo-sa-radom-na-podrucju-blockchaina-kriptovaluta/, (accessed 28th July 2018.)

309 See. 183

310 B.Lietar and J. Dunne, *"Rethinking money: How new currencies turn scarcity into prosperity",* Berret-Koehler Publishers, San Francisco, 2013, pp. 59, 68, 75-76, 199-202

two dimensions – regulation/ prohibition and acceptance/refusal of Bitcoin – may lead to four different scenarios.

A first, more optimistic scenario would be one in which, based on the assumptions that the market is regulated and controlled, cryptocurrencies gain an increasing social acceptance. [311] This would not mean that the fiat currencies suddenly become obsolete; rather, it would mean that cryptocurrencies, in particular bitcoins, become an integral part of the market in which both currencies work simultaneously. According to this scenario, hence, it will become crucial to implementing the focus over the exchange transactions, in order to discourage the illegal uses of bitcoins, in particular those related to the money laundering (and financing terrorism). Moreover, it would be desirable to develop new forms of digital payments, in order to both overcome the issues related to the difficulties of understanding the wallets' system functioning and consequently attract new cryptocurrencies' users.[312] It is clear that a growing cryptocurrencies' acceptance would change the concept of money in the modern world. It would entail a significant decrease of the governments' primacy in this sector, contributing also in depriving central authorities of some effective tools of monetary policies. Nevertheless, the need for a decentralization is increasingly growing, and it is enhanced by customers' will to find new ways of overcoming the problems related to digital payments, but without recurring to the contribution of the authorities.

A second, more realistic, scenario it is the one in which the virtual currencies will remain legitimate and controlled by the authorities, but they won't gain or lose their social acceptance.[313] Even if the actions taken by the Central authorities are more or less identical to those listed in the previous scenario, the interferences in the virtual currencies schemes may cause a higher grade of resistance of the society. This it could be expectable, in those situations in which new legal guidelines to comply with are infeasible for many, if not the totality, of the Bitcoin network users. The lack of a complete understanding of the Bitcoin phenomenon by the States, associated to the absence of constructive dialogues with the users, will create growing barriers between regulators and recipients.

311 A. Mikolajewicz-Wozniak and A. Scheibe, "Virtual currencies schemes- the future of financial services", in *Foresight,* Vol.17, No. 4, 2015, pp. 365-377.

312 Few examples of these innovations are: the development of Bitbill, the first Bitcoin produced in physical form developed as a device to carry value and that could be physically delivered; Bitcoin virtual credit cards; Bitcoin POS system – similar to a normal POS terminal – which could allow merchants to accept Bitcoin payments; bidirectional ATM's, designed to exchange fiat currencies into Bitcoin and vice versa.

313 A. Mikolajewicz-Wozniak and A. Scheibe, "Virtual currencies schemes- the future of financial services", in *Foresight,* Vol.17, No. 4, 2015, p. 373

A third, less realistic, scenario could be the one in which virtual currencies will became illegal but, at the same time, their social acceptance as a medium of exchange will increase.[314] Since cryptocurrencies are still perceived by governments as a serious risk to the economic stability, as well as a medium of incentivize criminal activities, States may proceed in declaring their illegality unilaterally. The consequences of this kind of scenario may be pretty dangerous, since cryptocurrencies can return to being used as a black-market currency. It is anyway evident that the vision of a complete decentralization and leaving the full emission of currencies in the hands of the users it is not an acceptable option on the part of the States. Therefore, the economic sector will remain strictly controlled and the cryptocurrencies will remain a solution attractive only for few, highly-specialized users.

A fourth scenario, the most pessimistic, is that in which the cryptocurrencies will be declared illegal and their social acceptance will decrease rapidly, leading to their complete disappearance. The eventual States' sanctions against Bitcoins or other cryptocurrencies will enhance society's worries concerning the adoption of these alternative forms of payments. Consequently, this will lead to a lack of confidence in the adoption of these new forms, followed by an obvious choice towards the most secure and legal fiat currencies. As a final result, cryptocurrencies will end up disappearing. This scenario is not only very pessimistic but, at the same time, also extremely unrealistic. The different States' approaches analysed in the previous paragraph show exactly the contrary. It would be possible only in the case of a radical shift in the Global tendencies which, at the present moment, seems to be almost impossible.

3.4 Final Considerations

Regardless of the scenario(s) that could, as it could t not, occur as a result of the different approaches adopted by European States, it is possible to draw the following conclusions. Undoubtedly, Bitcoin phenomenon and cryptocurrencies in general are the society's expression of the need for changes in the financial sector. If we also consider the numerous applications of block-chain technology in the most disparate fields – some of them already mentioned in the first chapter - it is easy to understand how the entire Bitcoin phenomenon is destined to leave a lasting legacy. It is now ten years since the Bitcoin network was born. For a good part of this decade, states have not worked to put adequate regulation on this phenomenon, for two fundamental reasons. The first, dictated by the arrogance, because they erroneously believed that it would be a phenomenon of

314 A. Mikolajewicz-Wozniak and A. Scheibe, "Virtual currencies schemes- the future of financial services", in *Foresight,* Vol.17, No. 4, 2015, p. 374

short duration and, above all, adopted only by a small circle of individuals. The second, based on the conservative idea of maintaining the centrality of power, which therefore would hardly be reconciled with trying to regulate a phenomenon that instead professes the subtraction of this power from the states in order to give it to the users. When the "Silk-road" case hit the headlines, showing openly how the underestimation of this phenomenon had been dangerous, the States began to work in order to contain the irregularities and the critical aspects of this new cultural paradigm. But, as it was shown in this chapter, States are having different ways of interfacing with this phenomenon and with the issues related to it.

Nowadays, especially in Europe, the path towards a regulation shared by all the States still seems very long and difficult. This will continue to create legal uncertainty both for those who have already interfaced in this world, investing also large sums of money, and for those who would like to approach it. Until now, no progress has been made to reduce the uncertainties linked to the Bitcoin phenomenon. This will contribute to worsening the already precarious human rights framework of the various right-holders present in the network. Financial regulators and policy-makers need to recognize that, when it comes to crypto-currencies, trying to set the exact contours of new rules is extremely hard. It was said that it is still debated whether a regulation should entail the whole system, the users or the (mis)uses of Bitcoins. Indeed, regulators should urgently acknowledge their own limits and trying to keep as much as possible an open mind when approaching to these new technologies. By simply banning or dismissing the technologies they are not familiar with, as well as not trying to force these new technologies and business models into their existing regulation, States will *de facto* excluding an increasing number of individuals from receiving a proper regulation, able to give them a proper juridical protection from all the possible violations of their rights. States need therefore to be more creative, even if that will require to take them out of their "comfort zone", in order to find a new, ongoing balance between old regulation and innovation. It is true that cryptocurrencies, in particular Bitcoin, poses a new whole series of risks; but they also offer the possibility to enhance the global financial system's efficiency. In this sense, hence, it becomes clear that States need to put in place new legal framework which will protect against risks and issues, but in such a way that does not attempt and block the unavoidable innovation of the Bitcoin phenomenon. The different approaches which have been described are showing the willingness of the States of adopting a new regulation which does not stifle the innovation, but which it will be at the same time able to protect Bitcoin users and workers by any possible form of deprivation from the enjoyment of their human rights.

Indeed, it should be considered that also some features of the cryptocurrencies schemes, once perceived as advantages, may one day turn out to be systems' shortcomings. One of them could be that stable money supply. Together with the growing demand, it has attracted investors who wanted to make a fortune in a short time. Unfortunately, if Bitcoin ultimate goal will be to became an alternative form of payment fully recognized and utilized, the major problem will rise up when the network users will stop to perceive bitcoins as a kind of investments and started to treat them as a medium of exchange. From this point of view, therefore, the European States, by virtue of their experience as an economic community firstly, and subsequently political, will have the great role of providing all the rules aimed at amortizing any economic and legal repercussions that users might have.

Finally, it is clear that an European shared answer it is only the first step. Regulatory responses could be more effective if they are coordinated on an international basis. A set of inconsistent regulatory responses at national level for problems of financial integrity and stability could not concretely address the risks connected to Bitcoin activities on the market, which are essentially international, as well as the risks that users, also distributed on international base, are facing. The issues faced by cryptocurrencies and Bitcoin are far from being virtual risks, but regulators should always bear in mind that their action must not erase the potential benefits of the new technologies they might regulate.

FINAL RECCOMENDATION: TOWARD NEW HUMAN RIGHTS-ORIENTED APPROACHES FOLLOWING THE CROATIAN AND SLOVENIAN EXAMPLES: THE CO-OPERATIVE APPROACH.

On the basis of what has been said in the previous paragraphs, it could be noted an overall tendency amongst the different approaches adopted by the European States. None of these approaches have been taken into account the self-regulatory and the self-enforcing aspects of the Network. Therefore, every regulation on Bitcoin, despite the positive innovation it might introduce, will be always perceived as a 'foreign body' by the same recipients of the regulations. Understanding that users' participation is essential in order to introduce a regulation that is also shared by them is a necessary step all governments should consider. In this sense, hence, the Croatian and the Slovenian examples constitute a valid basis from which propose a new, innovative approach which may involve actively the same rights-holders object of a possible regulation. These two States were the first to have the foresight to understand the potentials of the bitcoin movement, by introducing specific disciplines aimed at limiting both the possible negative uses of the same technology, and above all to reduce the possible violations of human rights given by the failure to act of the state. Moreover, Slovenia was one of the few states – together with Poland - who has expressly recognized mining as a proper activity within its legal framework.

The future approaches should therefore increasingly take into consideration this aspect of close cooperation with network users. This cooperation could be reflected in a wide range of positive innovations that could be introduced within the network in order to solve the main criticisms associated with it. In systems such Bitcoin, the delivery of decision coincides with its coercive enforcement. Bitcoin users may have the pivotal role in create a new form of awareness, which may lead to innovative and advanced insights for the Governments. Thus, States can propose new forms of regulations, but in an 'unusual' way. Instead of proposing Regulations which may affect the Network only from the outside, State should learn how to develop these regulations under the form of codes which may be programmed and implemented in the network by the same users- In this

way, hence, States could comply with the duties descending from the European Covenants, ameliorating the perception and implementation of the human rights within the Network. Moreover, States and users communities should propose the creation of *ad hoc* forum and meetings, aiming to strengthen these cooperation and to evaluate whether the human rights protection within the Network has been implemented or not and to discuss possible solutions to new criticisms and issues.

At the same time, also the users can have the role of enhance the protection of human rights in applying the principles descending from the Conventions, by relying on the self-enforcement characteristic. Bearing in mind the major issues faced in the enjoyment of human rights, this cooperative regulation can lead to different interventions. A first, necessary intervention is the one that covers the lack of guarantees over the bitcoins' ownership. This cooperation could be realized in two phases. The first phase should consist in the provision from the States of specific guidelines for the users. These guidelines have a dual purpose: to introduce knowledge of the essential elements of property rights within the network, on the one hand; on the other hand, to create a system of safeguards and guarantees able to cover the specific situation of the bitcoin network. The second phase should consist in an implementation of the protection of the ownership within the network, by proposing for instance the introduction of a new forms of guarantee.

It has been said that one of the key issues related to the right to property within the bitcoin network, lies in the question whether the right is applicable over the bitcoins or over the user' private key. Undoubtedly, therefore, these new forms of guarantee should take into account the problems deriving from the illegal appropriation of the private key. In this sense, it was recently proposed the idea of the creation of an 'multi-signature authorization system'.[315] By transferring their funds into a third-party wallet, users are able to protect themselves by implementing the system in which, to unlock the bitcoin transfer, it is necessary to use two separate private keys at the same time. The third part in question, which Ortolani calls 'escrow service provider',[316] will have the role of 'adjudicator'. If both the seller and the buyer involved in a bitcoin trade, fulfil their obligations, namely the simultaneous transfer of the cryptocurrency and its corresponding market value, the third party will authorize the transaction.[317] On the other hand, if disputes arise, namely failure to

315 P. Ortololani, The three Challenges of Stateless Justice, in *Journal of Dispute Settlement,* 2016, vol. 7, pp- 596-627,

316 *Ibid.*, p. 605.

317 P.Ortolani, Self-enforcing online dispute resolutions: Lessons from Bitcoin, in *Oxford Journal of Legal Studies*, 2015, pp. 1-35

fulfil the obligations, the escrow service provider will not authorize the transaction. This system, hence, can implement users' protection against fraudulent behaviours.

With reference to this last point, the creation of new 'figures' within the Network, States could have an important role. Moving conceptually from the recently created figure of the Data Protection Officer in the GDPR, States could propose the creation of a similar figure entitled to receive the complaints of users about the thefts of their bitcoin. This new figure will not be a physical entity, but it will assume the features of a software script to be implemented within the Bitcoin Network, to be then adopted and constantly improved by all users. The functions that could be assigned to this new figure/software are:

1) Collect the complaints and verify in the block-chain ledger the effective property right, claimed by the user deprived of his bitcoins illegitimately;

2) Verify within the block-chain ledger to which wallets the stolen bitcoins are transferred;

3) Proceed to block the wallets where the bitcoins have been transferred.

As a second facet of this innovations, a strict cooperation between users should lead to the introduction of new systems of restitution of the sums stolen from the original owners directly from the blocked wallet, following the Latin concept of *restitutio in integrum*. The major concerns related to this passage is the way in which it could be realized. As it was said many times, the only way in which it is possible to interrupt the flux of transactions' registrations within the block-chain is if the 51% of the users will co-operate to reverse or interrupt a transaction. This obviously could lead to further hacks of the system and therefore to uncontrolled results. It is clear that new methods for unlocking stolen bitcoins should be developed in the future, aiming at not compromising the integrity of the network but to grant, at the same time, an higher level of warranty for the users. Meanwhile, States should propose valid guidelines in order to speed up these processes. A concrete example it could be the creation of "frozen wallets", following the trend of the EU Directive 42/2014 "on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union".[318] These "frozen wallets" should store both stolen bitcoins and those bitcoins confiscated for established money laundering purposes. Then, these bitcoins should be or re-assigned to the previous owners or re-sold within the network.

318 EU Directive 42/2014, "on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union", retrieved at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0042&from=IT, accessed the 30 July 2018

Following these positive trends, users may well be encouraged by governments to collaborate in order to discourage the illegal uses associated with Bitcoins. In particular, users could cooperate with state authorities to report large bitcoin transactions made without the use of exchangers. In this way, the task of governments to verify the possible money laundering by associating suspicious activities with specific wallets could be facilitated by the network users themselves, eager to oust those "bad apples" that preclude a larger acceptance of bitcoins as an alternative form of payment. In this way, limitation of users' right to privacy would still be safeguarded, since users could perceive the real usefulness and foreseeability of these interferences. At the same time, if the misconceptions associated ro bitcoins will continue to decline, its acceptability as an alternative form of payment will continue to grow. Therefore, the need to improve the protection of all those who will begin to work more and more with the bitcoins will arise. A step that will therefore be inevitable will be to regulate the working categories of exchangers and, above all, *miners*. The latter will have an increasing importance, due their task of recording all the various bitcoins' operations within the block-chain ledger, making them even valid for VAT purposes. This will translate into potential gains for governments, which can also incentivize their fight against tax evasion. The possible introduction of all these aforementioned innovations could be saluted favourably from the users. They will play a pivotal role in all phases prior to the introduction, becoming at the same time both the recipients of the measures but also the main actors in the decision-making process.

At the same time, States should act to introduce specific regulations, both at national and European level, aimed at introducing certain legal remedies for:

1) *the theft of bitcoins*: in this sense, States should firstly regulate Bitcoins as form of property, according to their national definitions. States will take on the important role to clarify whether the right to property applies to the bitcoins themselves or over the private keys, Then, States should subsequently introduce specific remedies - such as the possibility for the robbed users, to make a complaint, even if against unknown persons. States will be able not only to cope with the current lack of regulation, which contribute in creating issues for the users, but also will comply with the specific obligations deriving from the ECHR and the EU Charter, as already described in paragraphs 2.5.1 and 2.5.2.

2) *the working positions of exchangers and Bitcoin miners*: the introduction within the national legal frameworks of these specific working categories will have the major value to eliminate the

possible causes of labour discrimination and of labour exploitation. Moreover, by introducing a legal discipline over these figures, it will be possible to create working associations of exchangers and *miners*, respecting the freedom of association expressly disciplined by article 92 ECHR. By introducing at an European level the professional figure of miners there will be also the fulfilment of the freedom to move, settle and provide services following the specific indications deriving from Article 15 (2) EU Charter.

3) *the circumstances, according to the ECHR and the EU Charter, providing the state with the entitlement to limit and interfere users' right to privacy*. On the basis of what has been said in the description both of the current European discipline towards the right to privacy and the corresponding States' obligations, it is clear that the current legal framework is not able to cope with the major issues descending from the illegal uses of Bitcoin. More specifically, States haven't been able until now to find a proper way in which they can limit and interfere directly with the right of privacy of the users. In this sense, the high level of secrecy of the users has constituted a problem for the States, because it is impossible to tracing the identity of users as it is masked by Bitcoin network's encryption. In this sense, the specific introduction of the concept of pseudonymisation in the Recital 26 of the GDPR, has marked an important step toward the comprehension of this technologic factor. In the next future, only through a strict cooperation with users and exchangers it will be possible both to limit bitcoins' illegal uses and to associate the pseudonymized wallet to a specific user.

Only through the cooperation with users and aiming to a progressive integration within the existing legal framework, it will be possible to discipline, or at least introduce those legal remedies, able to cope with the issues faced by Bitcoins' users. States have now the faculty to decide whether to remain anchored to the past or to adapt its regulative role to a new level, in which decision are made in conjunction with the same recipients, who will be those entitled to put into practice the shared regulation. This cooperation may, on day, have positive impact also in the decision-making phase at a political level. Anyway, if States want to achieve a real human-rights-oriented regulation, it is undeniable that taking seriously into account the necessities of the right-holders is the inevitable step in order to have a successful human rights based approach towards the issues related to the Bitcoin phenomenon.

BIBLIOGRAPHY

Books

- Bashar, N.D. & Chuen, D.L.K. "Bitcoin Minin technology", in D.L.K Chuen, "*Handbook of Digital Currency",* Academic Press, 29th April 2015
- Bercusson, B. 'European labour law and the EU Charter of Fundamental Rights', Brussels, ETUI, Brussels, 2002.
- Birks, P. "Before we begin: five keys to land law", in S. Bright and J. Dewar ed., "*Land Law: Themes and Perspectives",* Oxford, Oxford University Press, 1998
- Bonaiuti, G. 'Economic Issues on M-Payments and Bitcoin', in G. Gimigliano (eds) *Bitcoin and Mobile Payments*., Palgrave Studies in Financial Services Technology, Palgrave Macmillan, London, 2016
- Calder, A., *"EU GDPR A Pocket Guide"*, United Kingdom, IT Governance Publishing, 2016
- Castells, M. "*The Internet Galaxy: Reflections on the Internet, Business and Society*", Oxford University Press, London, 2001
- Chaum, D. "Blind Signatures for Untraceable Payments", In: D. Chaum, R.L. Rivest, A.T Sherman, (eds) *Advances in Cryptology*, Boston, MA, 1983.
- European Union Agency for Fundamental Rights, "*Handbook on European data protection law"*, Luxembourg, Publications Office of the European Union, 2014, p. 68, available at http://www.dvi.gov.lv/lv/wp-content/uploads/fra-2014-handbook-data-protection-law_en.pdf (accessed the 15 June 2018)

- Grabewarter,C., "*ECHR: a commentary",* C. H. Beck (eds), Bloomsbury Publishing PLC, 2014.
- Harris, D.J., O'Boyle, M., Bates E. et al., "*Harris, O'Boyle & Warbrick, 'Law of the European Convention on Human Rights*", Oxford University Press, ed. 2014, p. 245.261.
- Jenssen, T. B., "*Why Bitcoins Have Value, and Why Governments Are Sceptical?*", Master's thesis, University of Oslo, 14 May 2014, p.16, available at https://www.duo.uio.no/bitstream/handle/10852/40966/Jenssen-Torbjorn-Bull.pdf?sequence=7&isAllowed=y , (accessed the 25 April 2018)
- Keynes, J.M. "*A Treatise on Money"*, Harocurt, Brace, 1930, vol.1, pp. 5-6
- Lietar, B. and Dunne, J. *"Rethinking money: How new currencies turn scarcity into prosperity",* San Francisco, Berret-Koehler Publishers, 2013, pp. 59, 68, 75-76, 199-202
- Lim, J.W., "A facilitative Model for Cryptocurrency regulation in Singapore", in *Handbook of Digital Currencies,* Elseviert Inc., 2015pp. 361-381
- Nian, L.P. & Chuen, D. Lee K. 'Introduction to Bitcoin', in David Lee Kuo Chuen, H*andbook of Digital Currencies,* Elseviert Inc., 2015, pp. 6-30
- Pasquale, F. "*The black box society: the secret algorithms that control money and information*", 2015, Cambridge: Harvard University Press. from https://www-degruyter-com.uaccess.univie.ac.at/view/product/430038 (accessed the 11 June 2018)
- Swadling, W. 'Property: General Principles', in A. Burrows (eds). "*English Private Law",* Oxford, Oxford University Press, 2103, pp. 173-306
- Taylor, K.S. "Theories of Value", in K.S. Taylor "*Human Society and the Global Economy",* 2001, Online Economic textbooks, Suny-Oswego, Department of Economics, Chapter 6.

Journal Articles

- Artzrouni, M., "The mathematics of Ponzi schemes," in *"Mathematical Social Sciences",* 2009, vol. 58, no. 2, pp. 190–201.
- Barratt, M. 'Letters to the editor Silk Road: E-bay for drugs', in "*Addiction"*, 2012, vol. 107, pp. 683–684
- Baur, D.G., KiHoon, H., Lee, A. D., "Bitcoin: Medium of exchange or speculative assets?", in "*Journal of International Financial Markets, Institutions & Money"*, available at https://www-sciencedirect-com.uaccess.univie.ac.at/science/article/pii/S1042443117300720 , accessed the 6th May 2018
- Chaum, D., "Achieving Electronic Privacy", in *"Scientific American",* vol. 267, iss. 2, 1992, pp. 96-101
- Choo, K.K.R. "New payment methods: a review of 2010-2012 FATF mutual evaluation reports", in "*Computer & Security"*, vol.36, 2013, pp. 12–26.
- Clarke, R. "Dataveillance by Governments", in "*Information Technology & People"*, Vol.7, iss. (2), 01 June 1994, pp.46-85
- Collins, H. and Mantouvalou, V. 'Redfearn v. UK: Political Association and Dismissal', in "*Modern Law Review"*, 2013, vol. 73, p.909
- Dalhuisen, J.H. 'Legal Orders and Their Manifestation: The Operation of the International Commercial and Financial Legal Order and Its Lex Mercatoria', in "*Berkley Journal of International Law"*, 2006, vol. 24, pp. 129-141.
- De Filippi, P., "Bitcoin: a regulatory nightmare to a libertarian dream", in *Internet Policy Review*, March 2014, vol. 3, iss.2, p.6, available at https://policyreview.info/node/286/pdf, (accessed the 14 July 2018)
- de Terwangne, C., "*The Right to be Forgotten and the Informational Autonomy in the Digital Environment*", European Commission Joint Research Centre Institute for the Protection and Security of the Citizen, Luxembourg , 2013, p. 6, available at http://publications.jrc.ec.europa.eu/repository/bitstream/JRC86750/jrc86750_cecile_fv.pdf, (accessed the 13 June 2018)

- Di, L.," *Why Do I Need a Public and Private Key on the Blockchain?*", WeTrust, 30 January 2017, available at https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76, (accessed the 1st May 2018)
- Di Piero, C. 'Deciphering Cryptocurrency: Shining A Light On The Deep Dark Web', in "*University Of Illinois Law Review"*, vol.3, 2017, pp. 1267-1298
- Douglas, I.B et al., SPECIAL PROJECT: Self-Help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society, in "*Vanderbilt Law Review*," vol. 37, 1984, pp.845- 850.
- Fernandez-Bermejo, D.U., "The multilevel protection of the right of property in Europe", in "*China-EU Law Journal"*, vol.4, 2015, pp.75-103
- Filippone, R., "Blockchain and individuals' control over personal data in European data protection law", Master Thesis, Tilburg University, August 2017, p.5 available at http://arno.uvt.nl/show.cgi?fid=143638 (accessed the 10 June 2018)
- Grgic, A., Mataga, Z. & Others, "*The right to property under the European Convention on Human Rights, A guide to the implementation of the European Convention on Human Rights and its protocols*", Belgium, June 2007, available at https://rm.coe.int/168007ff55 (accessed the 16 June 2018)
- Herrera-Joancomartì, J. & Perez - Solà, C. "Privacy in Bitcoin Transactions: New Challenges from Blockchain Scalability Solutions", in *Modelling Decisions for Artificial Intelligence*, 2016, pp. 26-44, p. 38, available at https://link-springer-com.uaccess.univie.ac.at/content/pdf/10.1007%2F978-3-319-45656-0.pdf, (accessed the 19 June 2018)
- Ishikawa, M. 'Designing Virtual Currency Regulation in Japan: Lessons from the Mt Gox Case', in "*Journal of Financial Regulation"*, vol. 3, 2017, pp. 125–131
- Karg, M. "Anonymität, Pseudonyme und Personenbezug revisited?," in "*Datenschutz und Datensicherheit (DuD,)*" Vol.39, 2015, Issue 8, pp. 520-526
- Klein, D.B. and Robinson, J. 'Property: A Bundle of Rights?', in "*Econ Journal Watch*", September 2011, vol. 8, number 3, pp.193-204

- Kraft, D. 'Difficulty control for blockchain-based consensus systems', in *"Peer-to-Peer Networking and Applications"*, Vol.9, n.2, 2016, pp.397-413
- Kroll, J. A., Davey I.C and Felten, E. W "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries", in "*The Twelfth Workshop on the Economics of Information Security*", Washington DC, 11-12 June 2013, pp. 11-12;
- Kshetri, N. "Blockchain's roles in strengthening cybersecurity and protecting privacy", in "*Telecommunications Policy"*, 2017, vol. 41, pp. 1027-1038, purchased at https://acelscdncom.uaccess.univie.ac.at/S0308596117302483/1-s2.0-S0308596117302483-main.pdf?_tid=87610b2b-23a2-41c8-8348-87f20c5935aa&acdnat=1529909137_af87b6dee1ba12da0a5250fc746efb4e , (accessed 16th June 2018)
- Kshetri, N. "Will blockchain emerge as a tool to break the poverty chain in the Global South?", in *"Third World Quarterly",* 2017, vol. 38, iss.8, pp. 1710-1732.
- Lansky, J. 'Possible State Approaches to Cryptocurrencies', in "*Journal of Systems Integration"*, vol. 1, 2018, pp. 19-31.
-
- Low, K.F.K. & Teo, G.S. "Bitcoins and other cryptocurrencies as property?", in *Law, Innovation and Technology,* vol. 9, no. 2, 2017, pp, 235-268.
- Low, K.F.K. and Teo, E. 'Legal risks of owning cryptocurrencies', in *"Handbook of Digital Finance and Financial Inclusion"*, 2017, Vol 1, pp.225-248
- Mantouvalou, V., "The Protection of the Right to Works Through the ECHR", in "*Cambridge Yearbook of European Legal Studies*", vol. 16, 2012, pp. 313-332.
- Melkonyan,D. 'Concept of the rule of law in the case-law of the European Court of Human Rights', available at http://ysu.am/files/Davit_Melkonyan-1415702096-.pdf , accessed the 1st June 2018.
- Mikolajewicz-Wozniak A. and Scheibe, A. "Virtual currencies schemes- the future of financial services", in *"Foresight*", Vol.17, No. 4, 2015, pp. 365-377.
- Moore D. & Rid, T. "Cryptopolitik and the Darknet", in "*Survival, Global Politics and Strategy*", vol. 58, iss.1, 2016, p. 7-38.

- Moruby, M., Mackey, E., Elliot M. & Others, "Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK", in "*Computer Law & Security Review*", Vol. 34, iss. 2, April 2018, pp.222-233.
- Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System", available from https://bitcoin.org/bitcoin.pdf (accessed the 18th April 2018)
- Ølnes, S., Ubacht J. & Janssen, M. "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing", in "*Government Information Quarterly",* 2017, Volume 34, Issue 3, Pages 355-364.
- Ortolani, P. "Self-enforcing online dispute resolutions: Lessons from Bitcoin", in "*Oxford Journal of Legal Studies*", 2015, pp. 1-35
- Ortololani, P. "The three Challenges of Stateless Justice", in *"Journal of Dispute Settlement",* 2016, vol. 7, pp- 596-627.
- Raskin, M., "The Law of Smart Contracts", in *"Georgetown Law Technology Review",* vol. 304, 2017, p. 31
- Salmon, F., "The Bitcoin Bubble and the Future of Currency", 3 April 2013, available at https://medium.com/@felixsalmon/the-bitcoin-bubble-and-the-future-of-currency-2b5ef79482cb , (accessed the 6th may 2018)
- Savelyev, A. "*Contract Law 2.0: «Smart» Contracts as The Beginning of The End of Classic Contract Law*", 2016, National Research University Higher School of Economics (HSE) p. 10, available from https://wp.hse.ru/data/2016/12/14/1111743800/71LAW2016.pdf
- Savona, E. 'Organised crime numbers', in *"Global Crime",* vol. 15, 2014, pp. 1–9.
- Soska, K. & Christin, N. "*Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem*," available at https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf , (accessed the 8th may 2018)
- Sotiropoulou, A. & Guégan, D. 'Bitcoin and the challenges for financial regulation', in *"Capital Markets Law Journal",* Vol.12, No.4, October 2017, pp. 466-479

- Szabo, N. 1994, '*Smart contracts in Essays on Smart Contracts, Commercial Controls and Security*', retrieved at http://szabo.best.vwh.net/smart.contracts.html
- Szabo,N., "*Bit gold*", 27 December 2008, available from http://unenumerated.blogspot.com/2005/12/bit-gold.html , (accessed 23rd April 2018)
- Thorpe, C., Hammer, J., Camp, J., Callas J. and Bond, M. 'Virtual Economies: Threats and Risks'. in: Dietrich S., Dhamija R. (eds) *"Financial Cryptography and Data Security"*. FC 2007. Lecture Notes in Computer Science, vol 4886. Springer, Berlin, Heidelberg
- van der Sloot, B. 'A new approach to the right to privacy, or how the ECtHR embraced the non-domination principle', in *"Computer law &Security Review",* vol. 34, 2018, pp. 539-549.
- Vasek, M., Thornton, M., Moore, T., "Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem", in *"Lecture Notes in Computer Science"* (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol.8438, 2014, pp.57-71.

EU DOCUMENTS

- European Convention on Human Rights, Optional Protocol 1, adopted the 20 March 1952, Article 1
- European Convention on Human Rights, Art. 4
- European Convention on Human Rights, Art.8
- European Convention on Human Rights, Art. 11
- European Convention on Human Rights, Art. 14
- European Banking Authority , *'Opinion on 'virtual currencies'*, 4 July 2014, p. 13-14 purchased at https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

- EU DIRECTIVE 843/2018 “on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing”, article 8
- EU DIRECTIVE 843/2018 “on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing”, article 9
- EU DIRECTIVE 843/2018 “on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing”, article 12
- EU DIRECTIVE 843/2018 “on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing”, article 41
- EU Directive 42/2014, “on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union”, retrieved at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0042&from=IT, accessed the 30 July 2018
- EU Directive 40/2013 ‘on attacks against information systems and replacing Council Framework Decision 2005/222/JHA’
- EU Commission, “Report on Public Consultation on the IoT Governance’, 2013, available at https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation, accessed the 11 June 2018
- EU Charter of Fundamental Rights, article 7
- EU Charter of Fundamental Rights, article 8.
- EU Charter of Fundamental Rights, article 15
- EU Charter of Fundamental Rights, article 30
- EU Charter of Fundamental Rights, article 31
- EU Charter of Fundamental Rights, article 32
- ‘*Explanations relating to the Charter of Fundamental Rights’*(14/12/2007), OJ C 303, p7, when it comes to Article 17 it is immediately stated that “*This Article is based on Article 1 of the Protocol to the ECHR’.*, see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007X1214(01)&from=EN, (accessed the 6 July 2018.)

- (EU) REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data", and repealing Directive 95/46/EC (General Data Protection Regulation), GDPR, Recital 7, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, (accessed 12 June 2018)
- (EU) REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data", and repealing Directive 95/46/EC (General Data Protection Regulation), GDPR, Recital 26, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN,
- (EU) REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data", and repealing Directive 95/46/EC (General Data Protection Regulation), GDPR, Article 4, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN,
- (EU) REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data", and repealing Directive 95/46/EC (General Data Protection Regulation), GDPR, article 9, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN,
- (EU) REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data", and repealing Directive 95/46/EC (General Data Protection Regulation), GDPR, Article 17, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN,
- (EU) REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data", and repealing Directive

95/46/EC (General Data Protection Regulation), GDPR, Article 37, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN,

- (EU) DIRECTIVE 843/2018 "on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing", article 42
- (EU) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the "processing of personal data and the protection of privacy in the electronic communications sector", available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML, (accessed the 30th may 2018)

Court Sentences

- "*United States v. Ulbricht*", available at https://www.pbwt.com/content/uploads/2017/05/15-1815_opn.pdf, accessed the 8th May 2018.
- Court of Justice of the European Union, Case C-283/11, 2013, *Sky O¨sterreich GmbH v. O¨sterreichischer Rundfunk*, 22 January 2013, § 34
- Court of Justice of the European Union, *Google Spain v. AEPD and Mario Costeja Gonzalez*, 13th May 2014, §94 available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=IT
- Court of Justice of the European Union, Joined cases C-92/09 and C-93/02, *Volker und Markus Schecke GbR v. Land Hessen*, Opinion of Advocate General Sharpston, 17 June 2010, para. 71, available at http://curia.europa.eu/juris/celex.jsf?celex=62009CJ0092&lang1=en&type=NOT&ancre, accessed the 7th June 2018
- Court of Justice of the European Union, Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert*, judgment of 9 November 2010, §66.
- Court of Justice of the European Union, *Nold c. Commission*, No. 4/73,14 May 1974, p. 491, points 13 et 14.

- Court of Justice of the European Union, *Van Binsbergen*, No. 33/74, 3 December 1974, p. 129
- Court of Justice of the European Union., *Reyners*, No. 2/74, 21 June 1974, p. 631.
- ECthHR, *Papamichalopoulos v. Greece*, no. 14556/89, 24th June 1993, §. 43 and seq.
- ECtHR, *0 Matos e Silva, Lda. and Others v. Portugal*, No. 15777/89, 16 September 1996, §.75.
- ECtHR, *Angelova and Iliev v. Bulgaria*, No. 55523/00, 26 July 2007, §.117.
- ECtHR, *Anheuser-Busch Inc. v. Portugal*, No. 73409/01, 11 January 2007, §. 72.
- ECtHR, *Balan v. MDA*, No. 19247/03, 29 January 2008, §§.34 et seq;
- ECtHR, *Beyeler v. Italy*, No. 33202/96, 5 January 2000, § 100.
- ECtHR, *Dangeville v. France*, No.36677/97, 16 April 2002, §. 48.
- ECtHr, *Danilenkov a.o. v. Russia, No.* 67336/01, 30 July 2009, §76
- ECtHR, *Darby v. Sweden*, No. 11581/85, 23 October 1990, §.30;
- ECtHR, *Erkner and Hofauer v. Austria*, No. 9616/81, 29 September 1987, §74
- ECtHR, *Evaldsonn and O.v. Sweden*, No. 75252/01, 13 February 2007
- ECtHR, *F.Lombardo v. Italy*, No. 11519/85 & No. 12490/86, 26 Nov. 1992, §§16 & 17.
- ECtHR, Gasus Dosier-und Fördertechnik GmbH v. The Netherlands, No. 15375/89. 21 December 1992, para. 53.
- ECtHR, *Handyside v. The United Kingdom*, No.5493/72, 7 December 1976, §. 62;
- EctHR, *James and* Others v. *UK*, No.8793/79, 21 February 1986, §.46;
- EctHR, *Katte Klitsche de la Grange* v. Italy, No. 12539/86, 27 October 1994, §§. 42 and seq.;
- ECtHR, *Malone v. the United Kingdom*, No. 8691/79, 2 Aug. 1984, §. 67;

- ECtHR, *Marckx V. Belgium*, No. 6833/74, 13 June 1979, § 63
- ECtHR, *Négrépontis-Giannis v. Greece*, No. 56759/08, 3rd May 2011, §§. 97, 104
- ECtHR, *Öneryildiz V. Turkey*, No. 48939/99, 30 November 2004, §134
- ECtHR, *Paeffgen GmbH v. Germany*, No. 25379/04, 18 September 2007, § 78.
- ECtHR, *Pine Valley Developments Ltd. and Others v. Ireland*, No. 12742/87, 29 November 1991, § 56
- ECtHR, *Pretty v. UK*, No. 2346/02, 29 April 2002, §§ 88 et seq.;
- ECtHR, *Redfearn v. UK*, No. 47335/06, 6 Novmber 2012, §§ 43-48
- ECtHR, *Rees vs. UK*, 9532/81, 17 October 1986, § 37
- ECtHR, *Rotaru v. Romania*, No.28341/95, 4 May 2000, §.55.
- ECtHR, *Siliadin v. France*, No. 733316/01, 26 July 2005, §§. 84, 85 120 and ss.
- ECtHR, *Spadea and Scalabrino v. Italy*, No. 12868/87, 8 September 1995, §§. 33 and seq.
- ECtHR, *Sud Fondi S.r.l.a.o. v. Italy*, No. 75909/2001, 10th may 2012, par.109.
- ECtHR, Taşkın and Others v Turkey, No. 46117/99, 30 March 2005, §118
- ECtHR, *Thlimmenos v. Greece*, No. 34369/97, 6th April 2000, § 44;
- ECtHR, *Tkachevy v. Russia*, No. 35430/05, 14th February 2012, §.39.
- ECtHR, *Urbànska obec Trencianske Biskupice v. Slovakia*, No. 74258/01, 27 November 2007, §§ 120, 132 and seq.
- ECtHR, *Vilnes and o. v. Norway*, No. 52806/09 and 22703/10, 5 December 2013.
- ECtHR, *Young, James and Webster v UK*, No. 7601/76 and 7806/77, 13 August 1981, §.55;

Interviews

- Ametrano, F., Interview, Milan, 24th April 2018, Annex 2

- Bagella, M., Interview, Rome, 6th April 2018, Annex 1

Newspaper Articles

- "*Bitcoin Prices Rise; Spain Supports Crypto Regulation*", Cryptocurrency News, 1st June 2018, retrieved at https://www.investing.com/news/cryptocurrency-news/bitcoin-prices-rise-spain-supports-crypto-regulation-1474579, the 27 July 2018
- "*CNB: investendo in bitcoin, si assume completamente il rischio*", Monitor.hr, 24 September 2017, available at http://www.monitor.hr/hnb-ulaganjem-u-bitcoin-u-cijelosti-preuzimate-rizik/, (accessed the 28 july 2018)
- "*Croatia has allowed the Use of Bitcoins*", Coinspot.io, 16 December 2013, available at at https://coinspot.io/europe_and_russia/xorvatiya-razreshila-ispolzovanie-bitkoina/, accessed the 23 July 2018
- "*Croatian central bank establishes that Bitcoin is legal in Croatia*", Reddit.com, 10 December2013, https://www.reddit.com/r/Bitcoin/comments/1sjgby/croatian_central_bank_establishes_that_bitcoin_is/, (accessed 28 july 2018)
- *"How are new bitcoins created?"*, available at https://en.bitcoin.it/wiki/Help:FAQ
- "*Steps towards Self-Regulation in Croatia and Slovenia"*, Bitcoins.net, 18 February 2018 retrieved at https://www.bitscoins.net/steps-towards-self-regulation-in-croatia-and-slovenia/, 28 July 2018
- Bartoletti, M., Pes, B., Serusi, S. "*Data mining for detecting Bitcoin Ponzi schemes"*, 1st March 2018, available at https://arxiv-org.uaccess.univie.ac.at/pdf/1803.00646.pdf, accessed the 5 may 2018
- Beigel, O. *"What is a Bitcoin Wallet – Bitcoin Whiteboard Tuesday",* 99 Bitcoins, 4 July 2018, available at https://99bitcoins.com/what-is-bitcoin-wallet-bwbt-3/, (accessed the 1st may 2018)
- Bevand, M. 'Electricity consumption of Bitcoin: a market-based and technical analysis', available at http://blog.zorinaq.com/bitcoin-electricity-consumption/, (accessed the 11th may 2018)

- Business Dictionary, http://www.businessdictionary.com/definition/IOU.html , (accessed the 25 April 2018)
- Buterin, V. *Ethereum White Paper: A next-generation smart contract and decentralized application platform*., 2014 (Retrieved from https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, (accessed the 1st May 2018).
- Conti, M., "A Survey on Security and Privacy Issues of Bitcoin", in *IEEE Communications Surveys & Tutorials*, available at https://arxiv.org/pdf/1706.00916.pdf (accessed the 20June 2018)
- D. & A. Tapscott, '*The Impact of the Blockchain Goes Beyond Financial Services*', Harvard Business Review, 10 May 2016, available at https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services, accessed the 12th may 2018
- El Nakib, B. "*What is Bitcoins, How It Works? The Financial Action Task Force Issues Bitcoin Guidelines, warns about Money Laundering*", Compliance Alert, 15 February 2016, available at http://calert.info/details.php?id=781, (accessed the 2nd May 2018)
- EU network of independent experts on fundamental, *Commentary Of The Charter Of Fundamental Rights Of The European Union*, June 2006, p.90, available at http://www.pedz.uni-mannheim.de/daten/edz-k/gdj/06/network_commentary_final%20_180706.pdf, (accessed the 7th June 2018)
- Financial Action Task Force- FATF- , Report "*Virtual Currencies Key Definitions and Potential AML/CFT Risks*", June 2014, p. 7 available at http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (accessed the 15 June 2018)
- – FATF- *'Guidance for a risk-based approach to virtual currencies*', Paris, June 2015, p.4, available at http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf
- Greenspan, G. *'Beware of the Impossible Smart Contract', Blockchain news*, 12 April 2016, retrieved at http://www.theblockchain.com/2016/04/12/beware-of-the-impossible-smart-contract

- Groendahl, B. '*Austria Eyes Bitcoin Rules Based on Gold, Derivatives'*, Bloomberg.com, 23 February 2018, retrieved at https://www.bloomberg.com/news/articles/2018-02-23/austria-seeks-bitcoin-rules-based-on-gold-derivatives-controls, accessed 27 July 2018.
- Hajdarbegovic, N. "Financial Watchdog FATF Examines Risks of Digital Currencies", Coindesk, 30 June 2014, available at https://www.coindesk.com/financial-watchdog-fatf-examines-risks-digital-currencies/ (accessed the 2nd May 2018)
- Hansen, J.D. "*Digital Currencies: International Actions and Regulations"*, available at https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html#austria, (accessed the 21st July 2018.)
- Hansen, J. D. & Boehm, J.L., "*Treatment of Bitcoin Under U.S. Property Law*", March 2017, p.5, available at https://www.virtualcurrencyreport.com/wp-content/uploads/sites/13/2017/03/2016_ALL_Property-Law-Bitcoin_onesheet.pdf, (accessed the 3 July 2018)
- https://www.vocabulary.com/dictionary/fiat , accessed the 26th April 2018
- Huillet, M. "*Spagna: proposta a favore di criptovalute e blockchain ottiene l'unanimità del Congresso*", Cointelegraph.com, 31st May 2018, available at https://it.cointelegraph.com/news/spain-innovation-aimed-crypto-regulation-wins-cross-party-support-in-congress, (accessed 27 July 2018.)
- Jagati, S. '*Croatia Launches Self-Regulating Blockchain Organization*', Cryptoslate.com, 21 February 2018, available at https://cryptoslate.com/croatia-launches-self-regulating-blockchain-organization/, the 28 July 2018
- Jeffries, A. 'How to steal Bitcoin in three easy steps', *The Verge*,19 december 2013, https://www.theverge.com/2013/12/19/5183356/how-to-steal-bitcoin-in-three-easy-steps, accessed the 6th July 2018.
- Koumoullis, G. "Revisiting the 2013 banking crisis", CyprusMail Online, 22 October 2017, available from http://cyprus-mail.com/2017/10/22/revisiting-2013-banking-crisis/ (accessed 23rd April 2018)

- Kraft, D., "Difficulty Control for Blockchain-Based Consensus Systems". Master Thesis, University of Graz, 18 March 2015, p. 1 available at https://www.weusecoins.com/assets/pdf/library/University%20of%20Graz%20Blockchain%20Difficulty%20Control.pdf (accessed the 1 May 2018)
- Krancir, L. *"UBIK ha iniziato a lavorare attivamente nell'area della blockchain e della cryptovalute*", Crobitcoin.com, 15 February 2018, available at. https://crobitcoin.com/ubik-aktivno-krenuo-sa-radom-na-podrucju-blockchaina-kriptovaluta/, (accessed 28th July 2018.)
- Lyon, N. "*Belgium to Restrict All Transactions with Bitcoin*", Coinidol, 17th April 2017, available at https://coinidol.com/belgium-to-restrict-all-transactions-with-bitcoin, (accessed 27 July 2018.)
- Magliocco, P. "Quante monete come i bitcoin esistono?", La Stampa -Economia, 13 January 2018, available at http://www.lastampa.it/2018/01/13/economia/quanti-monete-come-i-bitcoin-esistono-UWXjyrQxYw37VNH7A97yqI/pagina.html, (accessed 23 april 2018)
- Maras, E., "Researcher Has Bitcoin Stolen off His Back in a Public Experiment", in *Crypto Coins News*, 11 November 2015, https://www.cryptocoinsnews.com/researcher-bitcoin-stolenoff-back-public-experiment/, Retrieved 6 July 2018.
- Martucci B., "*What Is Cryptocurrency – How It Works, History & Bitcoin Alternatives*", in Money Crashers, available at https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/ (accessed the 23 April 2018)
- McCook, H. 'Under the Microscope: The Real Costs of a Dollar', CoinDesk, 5 July 2014, available from https://www.coindesk.com/microscope-real-costs-dollar/, (accessed 11th may 2018)
- NBC New York, *"Schumer pushes to shut down online drug marketplace*", NBC New York, 5 June 2011, available at https://www.nbcnewyork.com/news/local/Schumer-Calls-on-Feds-to-Shut-Down-Online-Drug-Marketplace-123187958.html, (accessed the 8th may 2018).

- Norry, A. "*Bitcoin and Money Laundering: Complete Guide to Worldwide Regulations*", BlockOnomi, 2 July 2018, available at https://blockonomi.com/bitcoin-money-laundering/ (accessed 2nd May 2018)
- O'Neill, P.H., "*The Definitive History of Silk Road",* The Daily Dot, 11 October 2013, available at https://www.dailydot.com/crime/silk-road-drug-ross-ulbright-dread-pirate-roberts-history/, (accessed the 6th may 2018)
- Ou, E. "*No, bitcoin won't boil the Oceans*", Bloomber.com, 7 December 2017, available at https://www.bloomberg.com/view/articles/2017-12-07/bitcoin-is-greener-than-its-critics-think, accessed the 11th may 2018
- Silva, P. "*A European Data Protection Framework for the 21st century. Safeguarding Privacy in a Connected World*", available at https://hrmi.lt/wp-content/uploads/2016/11/Paolo-Silva_Presentation-Digital-Rights-Forum.pdf, accessed the 12 June 2018
- Thielman, S. *Silk Road operator Ross Ulbricht sentenced to life in prison*, The Guardian, 29 May 2015, available at https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced (accessed the 8th May 2018)
- Ulm, B. *Bitcoin ATMs boom: new locations*, Coin telegraph, 28 July 2014, available from https://cointelegraph.com/news/bitcoin-atms-boom-new-locations, (accessed the 3rd may 2018)
- Visser, L. "Why does Bitcoin have value and how is the price determined?", LUNO, 15 March 2017, available from https://www.luno.com/blog/en/post/how-bitcoin-price-determined, (accessed the 29 April 2018)
- UNODC, *"Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies"*, June 2014, p. 32, available at http://www.imolin.org/pdf/FULL10-UNODCVirtualCurrencies_final.pdf, (accessed the 2nd May 2018)

Annex 1- Interview with Professor Michele Bagella, former director of the Economy Faculty at the University of Roma, Tor Vergata.

Prof. Bagella, since the beginning you have always been against the widespread use and diffusion of the Bitcoin technology and bitcoins payments. Can you please tell me what are, in your personal point of view, the reasons why you believe that this technology is negative?

The first problem has to be traced back to the lack of control. We don't know who is entitled to control the issue of these rights in using bitcoins. While in the traditional fiat currencies case we use every day, the control starts by the central Bank (or by central Authority) and it develops through the lines of control supplied by the same central bank, this doesn't happen within the Bitcoin network. A second problem is the access to this technology. It is not easy for everyone to

get access to this technology, since not everyone is aware about how to enter inside this network. Furthermore, once inside, it is also very complicated to get out from this technology. This is valid also for what concerns the incomes obtained by the eventual upgrades of bitcoins value. A third problem is, when exiting from this technology, the necessity of taking into account the exchange rates. This means taking into account when it is the right moment to get out. Personally, hence, I see the whole Bitcoin phenomenon as a speculative movement, in which can withstand only those who are ready to accept the high level of risks related to the volatility and the value of the bitcoins. For sure, a great merit of bitcoins' success has to be attributed to the public opinion, which has seen it as an alternative coin, instead of perceiving it as a financial instrument.

In referring to the public opinion, do you believe that, before the speculative bubble of 2017, the widespread conception about bitcoins was negative, maybe due its original use within the deep web market- for instance in the silk road portal - for purchasing drugs or for recruiting assassins?

It was, indeed! It is clear that a non-regulated system allows, to those who have "problems" with the justice, to be used in an illegal way without the high risk of being investigated or arrested for illicit activities. A practical example could be the money laundering. If there are payment systems which allows to avoid the bank systems and the use of the fiat currency, the possibility of seeing from whom high sums of money are transferred and why it is very difficult. This lack of central control incentives those who wants to launder the money from their illegal activities. The latter, it has to be remembered, are already covered activities. If to these covered activities, we also add a "covered payment system", it is desirable at least a higher level of control and regulation.

Recently, in Italy, the Revenue Agency has introduced the obligation, for all Bitcoin consulting firms, to present a "know-your-client" format to all those who want to invest in the Bitcoin market. It is a questionnaire in which the potential investor must declare his name, his origin, his field of work, if he has criminal relationships, and why he is investing in bitcoins. Do you think that this could be a first step in order to introduce a regulation?

Indeed, this has to be considered as a first, important step. At the same time, this shows that the cryptocurrency ends up being an instrument between all the alternative electronic money which are under the control of the Central Authorities. If this will happen, in my opinion this will be good. But, in the case of Bitcoin, I have the impression that no one wants a central control.

The philosophy at the bottom of the Bitcoin movement is, indeed, to introduce a decentralized form of payment, without passing through central authorities or third parties.

But, most of all, the willingness of not passing through central controls. The system in which we make payments, with a regulated currency, is based on a set of rules and controls. This means that

there are international and national laws and rules which regulate all the aspects in the fiat currencies world. Something that is already beyond what is happening with Bitcoin. If there are blocks of email addresses within there are subjects who act in illegal fields, the compensations' operations can be easily realized. Hence, for this very reason. We have to be very cautious in using bitcoins as a form of payment.

Despite what you are saying, in Italy the number of merchants who accept bitcoin payments is growing rapidly. Furthermore, they believe that, thanks to the Block-chain and bitcoin transactions, it could be possible to use these systems for fighting taxes evasion, a sadly widespread phenomenon in Italy. What do you think about this?

If it will be like this, and all the people will use these technologies with this specific purpose, allowing also the authorities in verifying the regularity of all transactions, I welcome it. But, sincerely, I doubt that this could be the goal of the people who introduce these systems. I also doubt that these systems will develop in the way we expect, namely as an alternative, integrative payment system, but under the control of the authorities.

What do you think about the situation of the rights of the people who have chosen not only to invest in this sector, but also to work with Bitcoin operations and consulting. Since there is not a regulation able to discipline those rights and the insecurity of their work situation, how do you think it could be possible to reconcile the protection of these rights with the decentralized philosophy of the bitcoin movement?

Honestly, I don't know how to answer. In referring to the consulting, if we talk about well-known societies, the rights of the workers are safeguarded by the same norms applicable to normal societies who don't offer bitcoin consulting. If we talk about societies who are encouraging the labour exploitation, we are facing also a responsibility of the same exploited people.

In relation with what you have said about the labour exploitation, the block-chain technology has introduced a counter-trend innovation, the Proof of Work. So, if one hand there is not a shared regulation yet, on the other hand the right to work of the people involved in the block-chain is incredibly protected. What do you think about this?

I still don't know how it is possible to think about a system of control without a central authority. In the context of the work, there are two simultaneous responsibilities. On one hand, there is the producer's responsibility; on the other hand, the consumer's one. In this case, as long as there will be someone who will see its labour exploited, there will be for sure a responsibility of the same system who didn't' prohibit it since the beginning. In the context of Bitcoin, if the whole block-chain system would have been clear and transparent, consequently the whole compensation system

would have been known and this means that there will be a referent able to exercise a system of control upon the whole system. Until when this won't be possible, it will be only bartering economy, based on the exchange of values between individuals.

How do you see this technology five years from now?

I am not such an expert in technology so I can't make provisions about how this whole phenomenon will develop. For sure, it is undeniable that the technology will have more and more an important role in the society. In which direction? Only the future will tell us the truth.

Annex 2 – Interview with Professor Ferdinando Ametrano, professor of "Bitcoin and Block-chain Technologies" at Milano "Bicocca" University.

1). *Professor Ametrano, in the Italian academic world, you figure out as one of the strongest advocates of the Bitcoin and block-chain technology. Can you please tell me when, and how you begin in being interested in these technologies*?

In 2013 I was in charge of Fintec, the bank I was working for. I actually have heard about bitcoins before, and I had a natural empathy for currencies without a central bank, but without paying too much attention to it. In February 2013, I went to a two-day conference in Berlin and most of my questions had brilliant answers. Nonetheless, I was stubborn and I had to spend three or four months of hard, passionate study. I was sceptical at the beginning. I thought Bitcoin could not work, otherwise everybody else would have been talking about it. But, in the end, I had to give up. Bitcoin was working and could have been changing the history of money and finance. Since that moment, I have been dedicating myself for most of my time to study bitcoin and I become more

and more convinced that bitcoin is the digital equivalent of gold. For the first time in history, we have scarcity in digital realm. If we think about how relevant (physical) gold has been in the history of civilization of money and finance, we can understand how disruptive digital current of gold could be in the digital civilization of money and finance as well.

2). *Many of your colleagues are deeply critical towards this technology, for several reasons: from the lack of a central control, to the problems of access and withdraw from the network, not to mention the well-known criticisms about Bitcoin's speculative nature and its illegal-related use within the Deep-Web. How do you answer to this widespread criticism*?

They touch all multiple points. First of all, everything about bitcoin is about freedom. Nobody is forced to use bitcoin. So, this is very different from legal tender currencies which we are forced to use. Bottom line is if you dislike bitcoin, so don't use it. About being speculative investment. Price dynamic is how the market reaches consensus on the fair value of an asset. If an asset has something controversial, potentially disruptive, dramatically innovative like the digital equivalent of gold is clear that the process of assessing its price must be controversial, confused. In a world: volatile. So, Bitcoin volatility is natural. A practical example is Amazon. At its debut in 1997, Amazon was worth $ 1.40, it came in 1999 during the Internet bubble at $ 113, then collapsed a $ 5.51 in 2001 with a loss (peak-to-depression drawdown) of 95%; today it is worth more than $ 1400. Ten years later, we can say that e-commerce proposition was all relevant, despite back in the days was not clear at all. I am pretty confident that in 20 years down the road the relevance of digital gold will be clear to everybody but today is still a work in progress. The understanding is controversial and complex. Moreover, if something increases its value nine thousand times in seven years, such return is a compensation for huge risks. It must be. In finance there is no "free lunch". It's just a reward for the risk you have undertaken. The grey area of Bitcoin, used by crypto lockers and similar. The most relevant crypto locker so far was '*Wannacry*', which has collected something like $125.000. This phenomenon has not an economic interest in business. I am more inclined to look at them as part of the cyber war. Of course, I mean, bitcoin may be used for criminal activities. Criminals, however, use also GPS, Iphones, Internet, the aviation with commercial flight. Anything good, which has a physiological usage, can be used also in a pathologic way.

3). *In a recent interview, you have said that one of Bitcoin's major issue is its lack of fungibility. Do you think is a solvable problem from here to five years, for instance?*

Let's start defining what fungibility is. The key issue nowadays is that not all bitcoins are equal. For each bitcoin you can trace back its history. I might be willing in paying more for a bitcoin

which comes straight from the '*genesis block*', maybe just for collector reasons. Or I might be willing on paying more a bitcoin because it wasn't tainted by criminal usage. For the sustainability of digital scarcity experiment, bitcoin must become fungible or bitcoin must become equal. The golden atoms tell nothing of their history. They are indistinguishable from one another: even if a golden atom of my wife's wedding ring was involved in a bloody crime 300 years ago, my wife would know nothing about it and would be calm in bringing her ring at her finger. We need to preserve this kind of fungibility not just to help crime, but to help digital scarcity which will empower libertarian views and freedom processes. I do see that for bitcoin that is quite problematic, since they can not be designed from scratch once again. We have to live with deficits in its creation. What we can do is create a second layer, which in a way will mitigate bitcoin's problems. I am confident to the point of making almost of those problems disappear. We will always have the bitcoins' blockchain as a real time gross asset system which will be transparent to everybody's inspection and will remember the history and we will have this layer even with higher transactions volume which will respect privacy making bitcoin fungible. I think that is viable. The main alternative will be to start again from scratch but that will be really problematic. We don't have any guarantees that the second attempt of bitcoin experiment will have the same success of the first one. So, I think that the improvement of bitcoin protocol will be evolutionary without any dramatic start-over and I am confident it could be achieved in a five years' time-scale.

4). *The whole Bitcoin technology embraces a large amount of rights, disciplined both at an international and at a regional level. Some of these rights, such as the right to privacy and the right to work, have seen their implementation thanks to this technology. Other rights, such as the right to property, seem incredibly limited, due the lack of a reference legislation able to protect possible victims of fraud or robbery. In your opinion, despite the permission-less philosophy, which is at the base of Bitcoin network, don't you think that it could be possible to start a regulation process, at least about certain aspects, in order to improve the protection of these rights?*

I strongly disagree with the idea of bitcoin not helping with property rights. "Physical gold is a defence of property rights". This is the reason why governments and politicians have never loved gold. I think that the idea that bitcoins can be stolen from you or that bitcoin can be lost has to be framed if we think about an ounce of gold. If you lose your ounce of gold while you are on a transatlantic cruise, your gold is gone. You cannot recover that. If somebody steal your gold, you have not technical means to recover it back. Of course, you can address a judge, and I am pretty confident that if malicious agents steal someone's bitcoins, those agents can be persecuted. Of

course, bitcoins are digital, but this aspect does not mean that they can be stolen without any subsequent incrimination. So, I think that there aren't human rights which can be harmed by bitcoin. When it comes to the regulation, it depends on what we intend for it. When it comes to physical gold, it is not possible to regulate, for instance, the chemical aspects related to it, such as the way in which it rusts in a certain amount of time. For sure, you can regulate the way in which gold is used. When we talk of usage, it seems to me that bitcoin is in a certain way already regulated. If you accomplish any sort of crime using bitcoins, or diamonds, or British pounds, or Euros, or stock, or equities, this crime it has to be persecuted, no matter what currency you have used. Do we really need a special regulation for bitcoins? I don't think so. And I don't think what people really want to regulate. The current regulation pertains to the points of contact between legal tender currencies and bitcoin. And that is, in my opinion, legitimate, because wherever we have legal tender currencies, those are in real mode regulators. Bitcoin itself can not be really regulated. Technically it doesn't' have a governance body so there is nobody which could force bitcoin development in one direction. It was technically being designed in order to be resilient to any exogenous or regulation attack.

5). *Recently, the block-chain technology was used in some projects concerning human rights. I refer, in particular, to the WFP project of letting 10.000 refugees in a refugee camp in Jordan paying their food through a platform which follows the principles of block-chain or, again, the recent use of this technology to monitor last march 7th elections in Sierra Leone. What do you think about the impact that this technology may have in the human rights' protection*?

It may have a very good impact. But I think that non-monetary application of block-chain are nonsensical. In order to reach distributed consensus on a shared ledger you need economic incentives for the nodes to be honest. Otherwise, you can not solve problem which is known in computer-science as "*bizantinger* problem". In a circulus network where even one single node can be faulty or malicious, you can't reach consensus. Go figure on a ledger which should preserve economic value or voting results. You need to have a native digital asset who drives devoted to pay for decentralized consensus. So, there is no blockchain without Bitcoin. There is of course blockchain beyond bitcoin. There are blockchain applications which are basically notarization. I am not familiar with the voting experiment, but I can see that one pool provide cryptographic evidences of voting results on a blockchain in order to avoid to those declaration to not be tempted. Nut using blockchain for voting itself it implausible. I mean, nobody has really been able to provide with a clear case or way of using it. A centralized database with proper rewrite access to relevant parties can fulfil that, so I don't see a real application of the blockchain for that. Blockchain without

bitcoin is a chimera, because without it blockchain it won't last. Of course, notarization is a powerful idea because it can timestamp any data centre, any file, any declaration. Of course, timestamping declarations make it true and it is possible to recognize false or declarations. I think we are not ready yet, until when we won't familiarize with the idea of digital gold first.

6). *Why, in your opinion, despite the excellent potentialities of Bitcoin, there is still a widespread scepticism around this cultural innovation?*

Because Bitcoin is not a technology. This is why I don't like the so-called "Block-chain technology". Bitcoin it's mainly a cultural paradigm shift. Thanks to the ability of Nakamoto's consensus of solving the double-spending problem, we can now move from centralized security to decentralized security. This is absolutely different to what we have seen in the past centuries. When it comes to money, we elected the governance of money to be governed by the monopolies because, technically speaking, it was better to deal with them in order to have a well-ordered economy. These days that is not necessary anymore so we can experiment with private money and those private money can compete with the legal tender money, whether the latter doesn't approve this changing. And those who don't have that power, anyway, are not familiar with such different paradigm. Moreover, this paradigm shift has to prove its sustainability in time. Bitcoin has gone quite far in doing that. It's working without real problems in the last nine years. Of course, in ten years from now, it will be validated by twenty years of operational success. Only at that point, probably, most of the people will accept the idea that we don't need central governance in order to rule digital scarcity, and so freedom in inventing private moneys and the competition among private and legal tender moneys, which has been dreamed by Fredrick von Hayek, will be incentivized. So, this is not an anarcho-capitalist fight against the system, it is not necessarily a violent revolution, this is a liberal revolution.

7) Conclusively, how do you see this cultural paradigm shift from here to ten years? Do you think that this cultural gap that generates the scepticism can be overcome?

Yes, I am confident we will familiarize this cultural paradigm shift and this technological innovation. Nowadays, we make phone calls without completely understanding how the GSM system works. If someone before doing a call will be concerned about the sustainability about the GSM network, this will sound crazy. Of course, now there is a novel *de facto* around decentralization which makes most people uncomfortable, unfamiliar or sceptical about decentralized paradigm. Young people, millennials, they have no problem with the idea of a supranational money. As "emails" and Internet were not designed by postal offices or central phone authorities, why the

next transnational network of payment of the world should be designed by banks and governments? It's only natural that will be realized by that kind of permission-less innovation which is fast and efficient. By permission-less innovation I mean no central editorial control, no centralized security mechanisms, no barriers to enter, which are key characteristics of emails and internet, so far. We live in the first really global information economy. Such economy cries out for a supranational digital money and bitcoin is the most plausible answer right now.

ABSTRACT

In the past two years, the use of cryptocurrencies as alternative forms of payments has grown exponentially. The most famous example is represented by Bitcoins, whose value has increased so much to attract an ever-growing number of investors, attracted by the prospect of easy gains and in short times. The increase in the number of users was accompanied by an increase in potential violations of human rights. The purpose of this work is therefore to verify whether the regulatory framework in Europe is able to provide adequate protection for the exercise of the right to privacy, the right to property and the right to work within the Bitcoin network, or if it is necessary to improve it.

In order to verify this situation, this work will be divided into three different phases. A first phase will describe the entire Bitcoin network, its functioning, the associated criticisms and the positive aspects that encourage its use. The second phase will analyse the current regulatory framework in Europe, taking into consideration the States obligations deriving from the ECHR and the EU Charter, and describing the practical issues faced both by users in exercising their rights and by States in regulating this phenomenon. Lastly, there will be a comparative analysis amongst the different approaches European states are having toward the bitcoin phenomenon, to assess whether the choices made are actually human rights oriented. The results obtained will lead to conclude this work with recommendations about a new possible approach that states should adopt.

Keywords: Bitcoin, block-chain, right to privacy, right to property, right to work, ECHR, EU Charter of fundamental rights.

KURZFASSUNG

In den letzten zwei Jahren hat die Verwendung von Kryptowährungen als alternative Zahlungsmöglichkeiten stark zugenommen. Das prominenteste Beispiel hierbei sind Bitcoins, welche durch ihren stark gestiegenen Wert das Interesse vieler Investoren geweckt haben einfache Gewinne in kurzer Zeit zu machen. Mit der wachsenden Zahl an Bitcoin Nutzer_innen stieg jedoch auch das Risiko möglicher Menschenrechtsverletzungen an. Dementsprechend zielt die vorliegende Arbeit darauf ab darzustellen, inwiefern im Kontext von Bitcoin Netzwerken rechtliche Regularien auf europäischer Ebene in der Lage sind Menschenrechte zu schützen oder ob es Verbesserungsbedarf gibt. Hierfür werden das Recht auf Privatsphäre, das Recht auf Eigentum sowie das Recht auf Arbeit als Beispiele herangezogen.

Die vorliegende Arbeit untersucht dies in drei Teilen: Zuerst wird das Bitcoin Netzwerk im Allgemeinen beschrieben, seine Funktionsweise, die an ihm geübte Kritik sowie die positiven Aspekte, die es für seine Nutzer_innen so interessant macht. Im weiteren Verlauf werden die aktuell vorherrschenden rechtlichen Rahmenbedingungen auf europäischer Ebene unter Berücksichtigung der sich aus der Europäischen Menschenrechtskonvention sowie der Charter der Europäischen Union ergebenden Staatenverpflichtungen analysiert. Hierbei werden auch jene praktischen Aspekte aufgezeigt, die sich für Nutzer_innen hinsichtlich der Ausübung ihrer Rechte sowie für die Staaten hinsichtlich der Regulierung ergeben. Abschließend werden unterschiedliche Ansätze europäischer Staaten hinsichtlich Bitcoins miteinander verglichen um darzustellen, inwieweit diese menschenrechtsorientiert sind. Auf die Darstellung der Ergebnisse folgen Empfehlungen für Staaten hinsichtlich neuer Ansätze um ihren menschenrechtlichen Verpflichtungen nachzukommen.

Schlagwörter:
Bitcoin, Block-Chain, Recht auf Privatsphäre, Recht auf Eigentum, Recht auf Arbeit der Europäischen Menschenrechtskonvention, Charter der Europäischen Union, Menschenrechte