Master Thesis

On

The criminogenic potential of cryptocurrencies and their regulation in China and the European Union.

Claudia Germán Gómez

LLM Law and Technology 2023

Tilburg Institute for Law, Technology and Society (TITL)

ANR: 689217

SRN: 2080788

Thesis Supervisor: Dr. Brenda Espinosa Apráez

Second Reader: Abigaïl de Rijp LLM

Word Count: 13. 749.

Acknowledgments

First and foremost, I would like to thank my two thesis supervisors, Dr. Brenda Espinosa and prof. Abigaïl de Rijp for the time, the patience, the commitment and support they have given me throughout this thesis.

Furthermore, I would like to express my gratitude and appreciation to my parents and my grandmother for giving me the wings to fly and a soft place to land. I feel very fortunate to have the three of you. You have always believed in me, even when I did not.

I would also like to mention the rest of my family and friends, because they have given me the words of encouragement that I needed during this process.

While I feel that this thesis has been the result of a great personal and academic effort, I would not have been able to complete this journey without any of them.

Abstract

Cryptocurrencies are a phenomenon that has been gaining popularity since their emergence in 2008. As these cryptocurrencies become more and more popular, criminals have expanded their operations and moved into the lucrative world of cybercrime. Likewise, their modus operandi has become increasingly complex due to the development of these technologies, the number of jurisdictions in which criminals operate, and the volume of economic profits obtained from illicit activities. Consequently, this has raised a challenge for the different state actors aiming to dismantle criminal activity related to cryptocurrencies This thesis addresses the question of how different cultural and political regimes have tackled the same challenge through the role of law. For this purpose, the first thing to explore will be the reasons why these cryptocurrencies are so attractive to criminals. In doing so, the focus will be on China and Europe, their regulatory approaches, the grounds, and the potential consequences of such approaches.

Key Words: Cryptocurrency, Blockchain, Regulation, Ban, European Union, China, Criminogenic, Decentralization.

TABLE OF CONTENT.

1. Introduction ……1

1.1 Background……..……..1

1.2 Problem Statement ……..……..2

1.3 Literature Review…….……..4

1.4 Research Questions ……..……..7

1.5 Methodology …….……..7

1.6 Chapter Overview……..8

2. Understanding cryptocurrencies, blockchain technology and their potential criminal use……..9

2.1Cryptocurrencies: a worldwide phenomenon……...9

2.2 Blockchain technology ……...……..11

2.3 Criminogenic Potential……..……..14

2.4 Conclusion ……..……..18

3. Regulatory approaches to tackle the criminogenic potential of cryptocurrencies: The European Union (EU).……..……..18

3.1. Regulatory Background: The European Court of Justice's Ruling: Skatteverket v David Hedqvist. ……..……..19

3.2 The 5th Anti-Money Laundering Directive (5AMLD) ……..23

3.3 Market in Crypto Assets Regulation: The MiCA Proposal……..26

3.4 Member States' Regulatory Approach……...29

3.5 Conclusion ……...……..32

4. Regulatory approaches to tackle the criminogenic potential of cryptocurrencies: China……33

4.1 Background and Legal Status: The cryptocurrency ban in China……38

4.2 Money Laundering and Terrorism Financing Regulation……..39

4.2.1 The Anti-Money Laundering Law of the People´s Republic of China (Decree No. 1 of 2006 of the People's Bank of China). ……..41

4.2.2 The Counterterrorism Law of the People´s Republic of China (Order No.36 of the president of the PCR)……..43

4.3 Reg ulation regarding fraud and embezzlement offenses…….……45

4.3.1 Legal Interpretation (2022) No. 5 The Decision of the Supreme People's Court on Amending the Interpretation of the Supreme People's Court on Several Issues Concerning the Specific Application of Law in the Trial of Criminal Cases of Illegal Fund-raising. ……..47

4.4 Other regulatory initiatives: Techno regulation and awareness campaigns……48

4.5 Conclusion. ……..49

5. Conclusions. …….……..49

Chapter 1. Introduction

1.1.Background

The year 2008 was a turbulent time for modern history. In September of that year, the stock and the housing market crashed unprecedently, leading to a terrible financial crisis that hit the world and left millions of people unemployed, homeless, and without savings.[1] In the wake of the economic turmoil, a great sense of resentment and total distrust against financial and public institutions remained. [2] As a response, in October 2008, the paper '*A Peer-to-Peer Electronic Cash System*' was published under the pseudonym 'Satoshi Nakamoto', introducing humanity to the first ever existent cryptocurrency: Bitcoin. This publication presented Bitcoin as a digital and intangible currency characterized for being produced in a decentralized form (i.e., it is not backed by any government and does not rely on a central issuer). [3] Thus, bitcoin allowed transactions to be carried out securely without needing a financial intermediary or paying commissions.[4] [5] The idea behind Nakamoto´s paper was not so much focused on the creation and development of Bitcoin itself but on the urgent need for a new monetary system, totally different from the current one, to avoid the recurrence of potential financial crises that could resemble the one lived that year.[6]

The impact these technologies have had on society and the field of innovation has become so significant that cryptocurrencies and blockchain have expanded their scope of application, being employed in other areas such as managing medical history data, facilitating the voting process, and even in the creation of digital passports. [7] Unfortunately, there are two sides to every coin. As has occurred with other technologies, these can be beneficial or harmful to society according to the intention by which they are

1 W. Arner Douglas, 'The Global Credit Crisis of 2008: Causes and Consequences' [2009] 43(1) The International Lawyer - American Bar Association 91-136

2 Michael Comiskey and Pawan Madhogarhia, 'Unraveling the Financial Crisis of 2008' [2009] 42(2) PS: Political Science and Politics <https://www.jstor.org/stable/40647525> accessed 1 June 2022

3 Satoshi Nakamoto, 'Bitcoin: A Peer-To-Peer Electronic Cash System' (Bitcoin.org, 2008) <https://bitcoin.org/bitcoin.pdf> accessed 1 June 2022.

4"Bitcoin y Criptomonedas – Ese.cl" <https://www.ese.cl/ese/site/artic/20180514/asocfile/20180514111252/bitcoin_y_criptomonedas.pdf> accessed March 2, 2023.

5 Claudia Rello Gil, 'La Criptomoneda, Bitcoin', (Degree Final Dissertation, Universidad de Zaragoza, 2020)

6 Comiskey and Madhogarghia (3)

7 Rosic A, Blockgeeks and Baggetta M, "17 Blockchain Applications That Are Transforming Society" (BlockgeeksAugust 13, 2020) <https://blockgeeks.com/guides/blockchain-applications/> accessed March 2, 2023

used. Cryptocurrencies are no exception. Fraud, money laundering, or the financing of terrorism are some of the criminal offenses that have involved the use of cryptocurrencies as a criminal medium and have alarmed governments worldwide. [8] Human and fundamental rights violations, market instability, and national security hazards are some challenges countries must tackle. [9]

1.2 Problem Statement

While technological innovation has been fundamental to the progress of society, it has also raised profound implications for human rights and liberties. [10] Indeed, technology can be categorized as beneficial or harmful as determined by how they are used according to social norms, ethics, and laws. [11] Therefore, it is not shocking to assert that technology has been used for socially abusive or criminal purposes on countless occasions. [12] Nor is it a surprise that the technology that involves the enablement and evolution of crime presents new challenges that regulation must tackle. [13] As the introduction forewarned, cryptocurrencies and blockchain are no exception. Firstly, they have generated severe concerns at the global level due to their criminogenic potential, as they have been used in illicit activities, both as a tool for the commission of crimes and as the material object of these. [14] Secondly, cryptocurrencies have posed a regulatory challenge, as they lack a similar technology on which legislative precedents have been created.

Regarding the first matter, the criminogenic potential is primarily built on two properties that have made this technology attractive to criminals: pseudo-anonymity and decentralization (the absence of third-party intermediaries that control crypto-related activities).[15]

---

8 Europol, 'Europol Spotlight: Cryptocurrencies tracing the evolution of criminal finances' (Europol, 2022)
9 Susana Patricia Noriega Poletti, 'Regulación de las Criptomonedas para garantía de sus beneficios) Degree Final Dissertation, Universidad de los Andes, 2018)
10 Harvard university, 'Examining how technological advancements affect the future of human rights' (*Harvard University Carr Center for Human Rights Policy*) <https://carrcenter.hks.harvard.edu/technology-human-rights> accessed 1 March 2023
11 Sam McQuade, 'Technology-enabled Crime, Policing and Security' [2006] 32(ISSN-1071-6084) The Journal of Technology Studies <https://scholar.lib.vt.edu/ejournals/JOTS/v32/v32n1/pdf/mcquade.pdf> accessed 1 March 2023
12 Ibid.
13 Ibid.
14 David Pérez Medina, 'Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo' [2020] 10(10/2020) Boletín Criminológico, Universidad de Cádiz <file:///C:/Users/User/Downloads/Dialnet-BlockchainCriptomonedasYLosFenomenosDelictivosEntr-7701822%20(1).pdf> accessed 1 March 2023
15 L. Márquez-Legajo, 'Bitcoin, un análisis de los determinantes de su valor en Argentina' (Masters Final Dissertation, Universidad de San Andrés, 2018)

Firstly, anonymity is the leading factor for criminals to use cryptocurrencies. [16] Systems, such as Bitcoin, provide their users with a substantial amount of anonymity. While it is true that transactions are recorded in the network, blockchain technology does not trace and store the IP of the parties involved in the financial operation. Therefore, IP addresses are not attached to a person or an entity, which hardens traceability. [17] This attribute facilitates criminals to perform numerous illicit activities through the cryptocurrency networks without being caught by the enforcement authorities of each respective country. For instance, anonymity has been a critical feature in favoring the commission of criminal acts such as the financing of terrorism, money laundering, and currency trafficking. [18]

Secondly, complications arise from the decentralized nature of cryptocurrencies. Under the ideal of not needing a third party to carry out financial operations, cryptocurrencies are not issued or controlled by any authority, government, or central bank. Indeed, this technology aimed to allow users to interact directly with each other and the cryptocurrencies. Therefore, lacking a centralized and hierarchical system, the environment wherein these users interact lacks a regulatory framework.[19] Consequently, it implies two interrelated outcomes. First, some jurisdictions do not recognize cryptocurrencies as valid means of payment. Secondly, in the face of the non-regulation, non-recognition, and decentralization, no authorities are dedicated to prosecuting crypto-related crimes nor institutions that aim to compensate the victims, leaving them without redress. [20]

Regarding the second matter, cryptocurrencies posing several regulatory challenges, the following should be mentioned:

Firstly, this technology does not have a similar technological precedent on which legislators can rely. [21] Secondly, the blockchain and the functioning of cryptocurrencies are complex to understand without the necessary knowledge which can lead to a wrong

16 Simon Dyson and others, 'The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime' [2019] 1(5799) Computers and Society < https://doi.org/10.31585/jbba-1-2-%288%292018> accessed 1 March 2023
17Ibid.
18Pérez Medina(14).
19 Márquez Legajo (15)
20 Márques Legajo (15)
21 Miguel Ángel García ramos and Ricardo Rejas Muslera , 'Análisis del desarrollo normativo de las criptomonedas en las principales jurisdicciones: Europa, Estados Unidos y Japón' [2022] 35(N 1699-8154) Revista IDP <https://raco.cat/index.php/IDP/article/view/n35-garcia-ramos> accessed 30 March 2023

assessment of the risks they pose. [22] Thirdly, cryptocurrencies are a global phenomenon. Confronted with this lack of clarity, jurisdictions worldwide are taking different regulatory approaches from each other (e.g.: China and the European Union) aiming to legislate cryptocurrencies. Hence, it is a regulatory challenge to tackle the criminal use of a transboundary phenomenon when its mere notion is so opposite in different jurisdictions.[23] In the fourth place, decentralization challenges legislators as they must regulate a technology that intends to detach itself from any central authority or third-party intermediary. Since cryptocurrencies operate within an organized and centralized world, which functions through rules and laws regardless of any political organization, their regulation becomes problematic. [24] The nature of the technology is the main reason why it is not easy to fit into the existing legal framework. [25]

This thesis seeks to elucidate which regulatory approaches China and the EU have adopted to tackle challenges posed by cryptocurrencies. The focus is on these two jurisdictions, because they are two of the world's most significant economic powers and have taken different regulatory approaches.

1.3 Literature Review

Cryptocurrencies are not only seen as part of the computer revolution, but also, as a phenomenon that has altered the world of finances. [26] [27] On the one hand, an intangible object was given the chance of being an alternative to traditional money transfers.[28] Conversely, the world was getting ready to know the blockchain system through cryptocurrencies. [29] For the first time, Nakamoto introduced the first entirely

22 Bitcoin y Criptomonedas(4)

[23] Andrei Novikov, 'LEGAL REGULATION OF CRYPTOCURRENCIES AND APPLICABLE RISKS' [2018] 1(4) Eureka: Social and Humanities <https://doi.org/10.21303/2504-5571.2018.00690> accessed 30 March 2023

[24] García Ramos - Rejas Muslera (21)

[25] Galishchynska, 'Legal Regulation of Cryptocurrency Circulation in The World' [2019] 4(1) Analytical Law 246-249

[26] José Miguel Domínguez jurado, 'Blockchain y las criptomonedas: bitcoin' [2018] 10(2339-9546) Oikonomics <https://comein.uoc.edu/divulgacio/oikonomics/_recursos/documents/10/5_Dominguez-Garcia_Oikonomics_10_a4_cast.pdf> accessed 30 March 2023

[27]Manuel González-meneses, Entender Blockchain: UNA INTRODUCCIÓN A LA TECNOLOGÍA DE REGISTRO DISTRIBUIDO (2 edn, Aranzadi 2019)

[28] Sofia Naranjo Valencia, 'Desafíos jurídicos que implica el pacto de criptomonedas como medio de pago en la celebración de un contrato de compraventa civil Una mirada desde el neoinstitucionalismo' [2018] 50(1) Con-Texto <DOI: https://doi.org/10.18601/01236458.n50.07.> accessed 30 March 2023

[29] Teresa López gómez-cadiñanos, 'Criptomonedas y Blockchain' [2021] 1(1) Universidad de Oviedo <http://hdl.handle.net/10651/61506> accessed 30 March 2023

decentralized cryptocurrency, pseudo-anonymous, and fast transaction speed. [30] Based on the technical aspects of how blockchain works, it is easy to understand the trust it generates in its users. Indeed, the fact that it does not depend on an institution to support it gives the processes that use this technology significant freedom, both in its creation and implementation, not to mention that, in many cases, the fact of being able to circumvent control becomes the leitmotiv of some products. [31] However, this novelty is subject to problems. The introduction of blockchain and cryptocurrencies have generated a significant concern around the globe, as criminals have used them to perpetrate illicit activities. [32] Money laundering, fraud, or the online trade of illicit goods are some criminal uses criminals make of cryptocurrencies. [33] Their use has grown over the years in terms of volume and sophistication. [34] This criminality is associated with cryptocurrencies' architecture. [35] Indeed, the cryptocurrency phenomenon poses some regulatory challenges since the novelties it introduces are complex to integrate into the traditional legal framework and provide a suitable environment for criminals. [36] [37] Challenged by this, jurisdictions began to react and regulate cryptocurrencies. [38] Concerning the EU, there has been a move towards balancing technology development and mitigating adverse effects through various pieces of legislation. Conversely, China has decided to adopt a stricter approach than the EU: indeed, it has banned any economic activity related to cryptocurrencies. (See Chapters 3 & 4). [39] This research examines both jurisdictions, their

[30] Claudia Rello Gil, ' La criptomoneda, Bitcoin' [2020] 1(1) Universidad de Zaragoza <https://zaguan.unizar.es/record/88794> accessed 30 March 2023

[31] Victor García paramés, 'EL FUTURO DE LAS CRIPTOMONEDAS: PROBLEMAS REGULATORIOS Y SOLUCIONES INTERNACIONALES' [2020] 1(1) Universidad Pontificia de Comillas <https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/38987/TFG%20Garcia%20Parames%20Victor.pdf?sequence=1> accessed 30 March 2023

[32] Devika Pérez medina, 'Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo' [2020] 206(2254-2043) Boletin Criminologico: Instituto Andaluz Interuniversitario de Criminología <https://revistas.uma.es/index.php/boletin-criminologico/article/view/11283/11691> accessed 30 March 2023

[33] Europol(8)

[34]Europol, 'Internet Organised Crime Threat Assessment (IOCTA) 2020' [2020] 1(1) Europol Spotlight <https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf> accessed 30 March 2023

[35] Igor Makarov and Antoinette Schoar, 'Cryptocurrencies and Decentralized Finance ' [2022] 1061 (1682-7678) BIS Working Papers <https://www.bis.org/publ/work1061.pdf> accessed 30 March 2023

[36] Tamara Marquez-legajo, 'Bitcoin, un análisis de los determinantes de su valor en Argentina ' [2018] 1(1) Universidad de San Andres <https://repositorio.udesa.edu.ar/jspui/bitstream/10908/16022/1/%5BP%5D%5BW%5D%20T.%20M.%20AyPP.%20Lojo%20M%C3%A1rquez%2C%20Tamara%20In%C3%A9s.pdf> accessed 30 March 2023

[37] Europol(8)

[38] García Paramés (31)

[39] María José Granados Cataño, 'Uso y regulación de las criptomonedas en Estados Unidos' [2021] 1(1) Universidad Católica de Colombia

characteristics, and why these regulatory approaches have been taken as they are explored to understand what role each approach plays in the context of criminality.

It is important to note that many papers explore cryptocurrencies and how blockchain works. This research will focus on papers published by authors such as Gaggioli and Lee, focusing on how blockchain technology operates.[40] [41] In the case of cryptocurrencies, reference will be made to scholars such as Härdle, who explain the relevance of cryptocurrencies in the financial and technological sphere. [42] References will be made to reports from agencies such as Europol or Chainalysis, which provide information on regulation, crimes associated with cryptocurrencies, and the characteristics that make these currencies attractive to criminals. [43] [44] Among the gaps in the literature, it is possible to find that authors such as McQuade, or Pérez-Medina, that associate the characteristics of cryptocurrencies with the commission of crimes, focusing primarily on their anonymity. However, decentralization is an understudied phenomenon. There is barely any empirical literature explaining the implications of decentralized technology, even less so concerning how decentralization affects regulation. Nevertheless, it is a crucial element for cryptocurrencies' illicit use. In the same way that it is possible to associate the regulatory approaches in the EU and China, thanks to authors such as García-Gabilondo, who investigates the proposed legal regime in the EU, or as Sergeenkov does regarding

<https://www.researchgate.net/publication/351914805_Uso_y_regulacion_de_las_criptomonedas_en_Estados_Unidos> accessed 30 March 2023

[40] Andrea Gaggioli, 'Blockchain Technology: Living in a Decentralized Everything' [2018] 21(1) Cyberpsychology, Behavior, and Social Networking <DOI: 10.1089/cyber.2017.29097.csi> accessed 30 March 2023

[41] Kyle Lee, 'What Is Decentralization?' (*Studycom*, 24 March 2022) <https://study.com/learn/lesson/decentralization-concept-examples.html> accessed 7 June 2022

[42] Karl Wolfgang Härdle and others, 'Understanding Cryptocurrencies' [2018] 44(ISSN 2568-5619) International Research Training Group 1792 <https://deliverypdf.ssrn.com/delivery.php?ID=777119081090115117123006124070076029117046025068004010066118104028006104104102113119029035055009008044005105100112123024011127106071060023014123064103095041013005002090096097115071118111024105022103065092125122097095096160050710670860850 02&EXT=pdf&INDEX=TRUE> accessed 30 March 2023

[43] Europol (8) (34).

[44] Chainalysis, ´The 2022 Crypto Crime Report: Original Data and Research into cryptocurrency-based crime.' (February 2022) https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf > accessed 9 March 2023

China. [45] [46] Nonetheless, it is challenging to find comparative analyses of their respective approaches, especially in the context of the criminogenic potential of cryptocurrencies.

1.4 Research Questions

Against this background, the question this thesis explores is:

Faced with the criminogenic potential of cryptocurrencies, what are the regulatory approaches employed by the European Union and China to prevent and mitigate the commission of such crimes?

To answer the main research question, the following sub-questions must be considered first:

1. What are cryptocurrencies, and what does it mean they have criminogenic potential?
2. Which regulatory measures has the European Union proposed for tackling the illicit use of cryptocurrencies?
3. Which regulatory measures has the Republic of China proposed for tackling the criminal use of cryptocurrencies?

1.5 Methodology

This thesis primarily implements the method of doctrinal legal research. More precisely, a collection and analysis of the most relevant juridical sources. It discusses a series of legal authorities, from case law to substantial law, aiming to clarify each jurisdiction's regulatory positions and how they apply to cryptocurrency. [47] [48] While it is true that at the beginning of the thesis, a literature review is performed to explain cryptocurrencies and the hazards they pose; still, the remainder of the research will explore the different

[45] Maria Gabilondo García, 'REGULACIÓN DE LOS CRIPTOACTIVOS Análisis del régimen jurídico propuesto en la UE para los activos digitales, y del régimen aplicable actualmente a los DLT Tokens' [2021] 1(1) Universidad Pontificia de Comillas <https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/48232/TFG%20-%20Gabilondo%20Garcia,%20Maria.pdf?sequence=-1> accessed 30 March 2023

[46] Andrey Sergeenkov, 'China Crypto Bans: A Complete History' (CoinDesk, 9th March) <https://www.coindesk.com/learn/china-crypto-bans-a-complete-history/> accessed 30 March 2023

[47] Kosta E, "Masterclass in Interpreting Case Law and Comparative Law : Doctrinal Legal Method "(Researching Law and Technology September 22, 2020)

[48] Reimann M and Zimmermann R, *The Oxford Handbook of Comparative Law* (Oxford University Press 2019)

regulatory instruments of the two jurisdictions. In the case of the European Union, the focus will be on legal sources such as the 5th Anti Money Laundering Directive, the proposal for a Market in Crypto Assets Regulation, or the European Court of Justice's Ruling: *Skatteverket v. David Hedqvist.* [49] [50] [51]On the other hand, in the case of China's regulatory approach, the analysis will primarily focus on the rationales and consequences of the Announcements made by the People's Bank of China (PBOC) — the state authority responsible for the country's monetary policy and its corresponding regulation — In particular, the analysis will focus in laws and governmental announcements for which China banned cryptocurrencies such as: '*Announcement of Preventing Risks of Bitcoin by People's Bank of China, Ministry of Industry and Information Technology, China's Banking Regulatory Comm. and Other Departments'* and the *'Announcement of the People's Bank of China, the Office of the Central Leading Group for Cyberspace Affairs, the Ministry of Industry and Information Technology and Other Departments on Preventing the Financing Risks of Initial Coin Offering.'* [52]

This research incorporates legal developments up to [May 17th, 2023].

1.6 Chapter Overview

Chapter 2 focuses on cryptocurrencies, how blockchain technology operates, their main characteristics, and their relationship with criminality. This is crucial to establish a basic knowledge of how cryptocurrencies work, as is functioning is complicated for the average citizen. Chapter 3 analyzes the main regulatory tools enacted by the EU regarding

[49] Judgment of the Court (Fifth Chamber) of 22 October 2015 Skatteverket v David Hedqvist Request for a preliminary ruling from the Högsta förvaltningsdomstolen Reference for a preliminary ruling — Common system of value added tax (VAT) — Directive 2006/112/EC — Articles 2(1)(c) and 135(1)(d) to (f) — Services for consideration — Transactions to exchange the 'bitcoin' virtual currency for traditional currencies — Exemption Case C-264/14 https://curia.europa.eu/juris/liste.jsf?num=C-264/14

[50] Directive (EU) 2015/849 of the European Parliament and of the Council of of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ 2 141/74

[51] i.) Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology. ii.) Proposal for a Regulation of the European Parliament of the Council on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (known as the Resilience Proposal or DORA); iii.) Proposal for a Regulation of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/234.

[52] P, "Public Notice of the PBC, CAC, MIIT, SAIC, CBRC, CSRC and CIRC on Preventing Risks of Fundraising through Coin Offering" (*The People´s Bank of China*, 8 de septiembre de 2017) <www.pbc.gov.cn/english/130721/3377816/index.html> accedido el 18 de junio de 2023

cryptocurrencies. Chapter 4 will focus on China´s regulatory approach. Finally, Chapter 5 presents the main conclusions from this research.

Chapter 2. Understanding cryptocurrencies, blockchain technology, and their criminogenic potential.

As Chapter 1 already highlighted, since the publishing of Nakamoto's whitepaper '*Bitcoin: A Peer-to-Peer Electronic Cash System*,' crypto assets have become a global phenomenon that has transcended beyond the financial sphere and now is being implemented in other areas of daily life.[53] Nevertheless, despite this rise in popularity, and the attempt of technology scientists to transpose cryptocurrencies into other areas of life, its functioning is still an enigma for the population unfamiliar with the technicalities of the financial and technological fields. [54]

2.1 Cryptocurrencies: a worldwide phenomenon

The notion of cryptocurrency is a complex concept. When Nakamoto introduced cryptocurrencies to society, 'he' defined them as a *'peer-to-peer version of electronic cash (....) that allows online payments to be sent directly from one party to another without going through a financial institution. '* [55] [56] While this is the initial notion of cryptocurrency, it remains complex for the average person unfamiliar with computing or the financial sector. Therefore, aiming to complement this concept of cryptocurrency, the European Central Bank provided a far more comprehensive form to describe them:

'Cryptocurrencies are digital tokens that can be exchanged electronically and do not exist in physical forms (...) they are speculative and not issued by central public authorities, being created and kept track by a network of computers using mathematical formulas, rather than by a single authority or organization.' [57]

---

[53] For instance it is being used on the health and medical spheres by implementing blockchain technology on the usage of medical-record systems.

[54] Wolfgang Härdle and others, 'Understanding Cryptocurrencies' [2019] 44(2568 -5619) International Research Training Group 1972 <https://ies.keio.ac.jp/upload/20191125econo_Wolfbang_wp.pdf> accessed 4 November 2022

[55] Nakamoto (3).

[56] Nakamoto(3)

[57] European Central Bank, 'What is bitcoin?' (*European Central Bank Eurosystem,* 13 February 2018. (Updated on 14 July 2021)) <https://www.ecb.europa.eu/ecb/educational/explainers/tell-me/html/what-is-bitcoin.en.html> accessed 30 March 2023

Therefore, cryptocurrencies, such as Bitcoin, are digital assets that, like any other traditional currency, can be exchanged and traded. Nevertheless, the main difference is that cryptocurrencies are outside of the control of governments and financial institutions. [58] Therefore, the defining characteristic is their organic and decentralized nature. Thus, they are not issued by any central authority, so they are theoretically immune from government interference or manipulation. [59] Along with decentralization, other distinguishing features of cryptocurrencies are their security and pseudo-anonymityThese three features are explained in more detail hereunder:

1) Decentralization: Platforms like Bitcoin cut out the intermediaries. [60] The currency, in this case, trusts the validation of transactions, i.e., users trust the blockchain technology behind Bitcoin instead of trusting in an economic institution. As with traditional currencies that are traded digitally, cryptocurrencies also have a usage in e-commerce. The only difference is, unlike fiduciary money, no institution controls the network of assets. An algorithm controls its availability; anyone with internet access can use it. [61] Given that cryptocurrencies are ungoverned, decentralization reduces financial costs and facilitates the flow of capital. Therefore, no laws apply to the network. Theoretically, cryptocurrencies are not subject to any jurisdiction because their jurisdiction is *'all internet, all over the world.'* [62]

2) Level of Security: Blockchain technology provides high security to the currencies. Indeed, it offers high resistance to potential attacks against the system. [63] For instance, Bitcoin counts with robust cryptographic backing that protects the network from counterfeiting. Compared to the technology used by banks and credit cards, the Bitcoin protocol is many times more secure. [64] Bitcoin and other currencies are mainly based on asymmetric cryptography, by which every Bitcoin stored in a wallet

[58] Carlos Almarcha Navidad, 'Bitcoin, Oro Electrónico' (Degree Final Dissertation, Universidad de Ciencias Sociales y Jurídicas de Elche, 2015)
[59] Andrea Gaggioli, 'Blockchain Technology: Living in a Decentralized Everything' [2018] 21(1) CyberSightings <DOI: 10.1089/cyber.2017.29097.csi> accessed 7 June 2022
[60] Ibid
[61] David Lee and others, 'Cryptocurrency: A new investment opportunity?' [2018] 20(3) Institutional Knowledge at Singapore Management University <10.3905/jai.2018.20.3.016> accessed 7 June En 2022
[62] Lee (41)
[63] A Bartolomeo, ') Introducción a la tecnología Blockchain: su impacto en las ciencias económicas' (B Digital Mimeo, N/D) <https://bdigital.uncuyo.edu.ar/objetos_digitales/15304/14.-introduccinalatecnologia.pdf> accessed 7 June 2022
[64] J. Khangura and J. Arora, "A Study on Security Threats to Blockchain & Cryptocurrencies," *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, 2021, pp. 1560-1564, doi: 10.1109/ICAC3N53548.2021.9725412.

generates protection through public and private keys. Although this technology is still hackable, it would take all the processing power of all the computers existing today, together with an immeasurable number of years, to have the minimal possibility of breaching the network. [65]

3) Pseudo-anonymity: One of the most significant doubts around crypto assets is whether these currencies are anonymous. [66] The answer will be: 'not in its totality, but to a certain degree.' Transferring personal data to create a wallet and conduct transitions is unnecessary in these networks. What is necessary is a pseudo-random identifier so it can be associated with that wallet. [67] People can hide behind their wallets to prevent others from knowing their identity or geographic location. [68] Furthermore, these wallets are part of blockchain technology; therefore, any transaction along two wallets will be recorded on the system due to its public nature. Anyone on the network can monitor the transactions made in the system, including past transactions associated with the user's wallet. [69] No one knows who is behind the wallet, and transactions do not show who the sender and receptor are; however, each transaction made will be available to the public. [70] Here is the topic of debate: on the one hand, identifying the person who controls the wallet is extremely challenging, while on the other hand, there are no financial movements that a user can keep secret or hide from public view. Indeed, anonymity is one of the main problems for regulation, as they are an intrinsic part of how cryptocurrencies operate, many people can hide behind it. Including criminals. [71]

2.2 Blockchain Technology

[65] Ibid
[66] M Harrigan, 'An Analysis of Anonymity in the Bitcoin System' [2012] 3(1) 11Clique Research Cluster, Complex & Adaptive Systems Laboratory, University College Dublin, Ireland <10.1109/PASSAT/SocialCom.2011.79> accessed 7 June 2022
[67] M Möser, 'Anonymity of Bitcoin Transactions an Analysis of Mixing Services' (*University of Münster*, 2013) <https://www.wi.unimuenster.de/sites/wi/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf> accessed 7 June 2022
[68] Patricia Bazan and others, 'Análisis del anonimato aplicado a criptomonedas' [2019] 14(18) Congreso Argentino de Ciencias de la Computación CORE <https://core.ac.uk/download/pdf/296434137.pdf> accessed 5 November 2022
[69] Ibm, ' What is blockchain technology? ' (*IBM*, N/D) <https://www.ibm.com/topics/what-is-blockchain> accessed 8 June
[70] Ibid
[71] Europol (8).

In the development of virtual currencies, blockchain emerged, becoming one of the most innovative technologies of our time. [72] Although its first application arose in response to the problem of double spending associated with Bitcoin in 2009, blockchain will have expectations for application in other areas such as transportation or food security. [73]

Blockchain works as follows:

The functioning behind cryptocurrencies consists of a network of thousands of computers called nodes. [74] Blockchain technology functions as a large accounting register. It is composed of a database where all transactions are recorded, including all the input and output data of the people involved and the value of each transaction. [75] For clarification, in blockchain, the transaction is the core element. However, each transaction can be divided into three parts:

1. An address of the person issuing the transaction and a destination address to whom the transaction is addressed.
2. The amount of Bitcoin to be sent.
3. The digital signature by which the recipient knows who is sending the Bitcoins. This part is crucial because it is related to the validation of the transaction by the Bitcoin network. [76]

All these data are stored in the blockchain, encrypted through a cryptographic hash. This mathematical algorithm transforms an arbitrary block of data into new series of characters with a fixed length. [77]

[72] Double spending is an attack any cryptocurrency is susceptible of suffering. It implies that any currency can be duplicated, therefore the same currency could be spent in more than one occasion. Blockchain technology avoids this problem by using a peer-to-peer network technology combined with public key cryptography.

[73] Bit2me, 'What is double spending' (*Bit2me Academy*, N/D) <https://medium.com/@ipspecialist/how-blockchain-technology-works-e6109c033034> accessed 12 June 2022

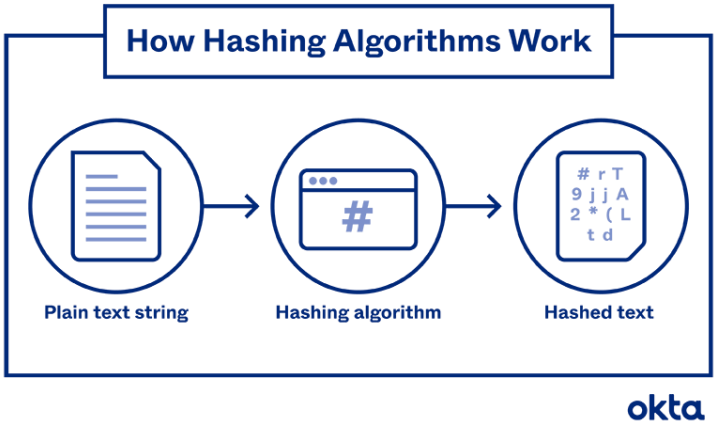
[74] Ip specialist, 'How Blockchain Technology Works' (*Mediumcom*, 15 October 2019) <https://medium.com/@ipspecialist/how-blockchain-technology-works-e6109c033034> accessed 12 June 2022

[75] Ibid

[76] Ibid

[77] Brian Donohue, 'The Wonders of Hashing' (*Kaspersky Daily*, 10 April 2014) <https://www.kasersky.com/blog/the-wonders-of-hashing/4441/> accessed 8 June

Illustration 1: Hashing Algorithm Overview [78]



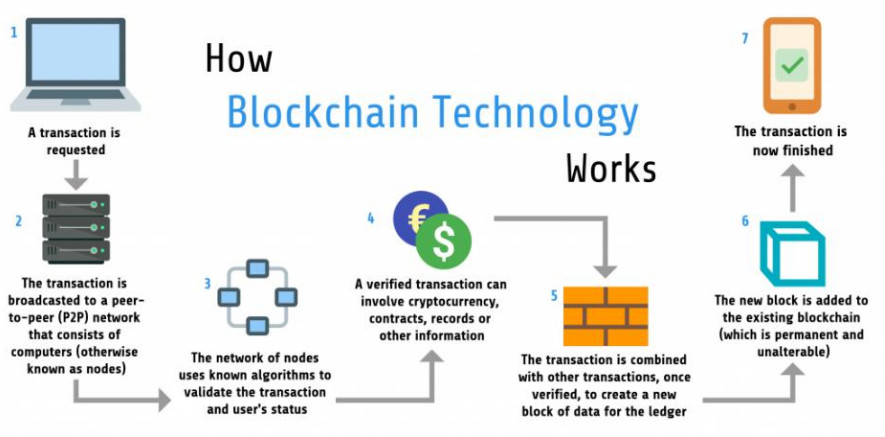
Then, that data is distributed in a network of nodes, each with an identical copy of that ledger. The fact that the web is decentralized brings some complications to managing the content since that data is distributed across all nodes. The network has as many copies of the data as users are in the network. For that reason, the role of blockchain is so crucial. When the transaction arrives at the node, it tries to build a block with the previous transactions. All the nodes in the network must solve a mathematical challenge (*proof-of-work),* and the first node that succeeds will form a block, becoming part of the chain of blocks (from here, the name blockchain). [79] The other attempts from the other nodes are discarded.

Once the block has been validated, it will be copied to the entire network, so everyone has the exact copy of the blockchain. This technology makes the network more secure concerning its content and data manipulation while generating higher trust. From the time of each transaction, each participant oversees the verification and authentication, making accessing or tampering with the transaction information very difficult. [80] [81]

[78] Okta, [image of} 'How Hashing Algorithms Work' (*Okta,* 2 February 2023) <https://www.okta.com/identity-101/hashing-algorithms/ > accessed 8 June
[79] Ibid.; IP Specialist (35)
[80] Bartolomeo A, Machin U. G, 'Introducción a la Tecnología Blockchain: Su impacto en las ciencias económicas' (Dissertation, N/D).
[81] A transaction example:

If A wants to send X Bitcoins to B, A must first connect to a node in the Bitcoin network. When sending the transaction, the node that receives it stores it and sends it to the nearest nodes. Then, the transaction goes through all the nodes in the network. And at some point, that transaction will be available at the node closest to the recipient. The recipient must check his nearby nodes to see any transactions for him. In this case, he will see a transaction from A with a certain number of Bitcoins and that this transaction has been validated by all the other nodes in the network.

Illustration 2: How blockchain technology works [82]



2.3 Criminogenic Potential

In 2021, an estimated 14 billion dollars were transacted from cryptocurrency-based crimes. [83] [84] Of that figure, 8.6 billion were related to money laundering activities, 2 billion in darknet markets, 180 million in ransomware, 7 million in scams, 4 million in stolen funds (through malware such as Trojans), and 1 million in terrorism financing. [8586] Consequently, it is a fact that cryptocurrencies have criminogenic potential.

The science of criminology defines criminogenic potential as the elements susceptible to producing crime, or that tend to originate criminality.[87]

While this term is usually applied to explain human criminal behavior and the factors that propel a person to offend, scholars such as José Agustina have extrapolated it to the

[82] IP Leaders, [image of} 'How Blockchain Technology Works' (*IP Specialist,* 15 October, 2019) < https://medium.com/@ipspecialist/how-blockchain-technology-works-e6109c033034> accessed 8 June
[83] IGaggioli (40)
[84] This figure refers to data from more than 60 countries, including Bulgaria, Russia, the United States, Ukraine, Romania, China, the Philippines, the United Kingdom, Morocco and Lithuania.
[85] (The remainders correspond to other offenses, such as those involving NFTs). Ibid
[86] NFT stands for Non-Fungible Token. Tokens are units of value assigned to a business model. They are digital assets certified by blockchain technology. The cryptography of these tokens is what makes these assets unique: no two are alike, and they cannot be exchanged with each other. This make it possible to prove that the person who has purchased it the sole owner of it. Matesanz Vanesa, 'NFT: qué son, cómo funcionan y cómo invertir' (*Finect*, 9 de agosto de 2022) <https://www.finect.com/usuario/vanesamatesanz/articulos/nft-como-funcionan-como-invertir#:~:text=Los%20NFT%20o%20'tokens'%20no,comprado%20es%20su%20propietario.> accessed 10 March 2023
[87] Hikal Carreón and Wael Sarwat, 'Revisión teórica a la génesis de la conducta criminal' [2017] 20(1) Revista Electronica de Psicología Iztacala <https://www.iztacala.unam.mx/carreras/psicologia/psiclin/vol20num1/Vol20No1Art11.pdf> accessed 3 March 2023

technological field.[88] Agustina associated the criminogenic potential with the own architecture of the Internet. He recognized that the characteristics of the Internet were the elements that made it conducive for a criminal to choose the Internet as the medium to commit a crime. Furthermore, Agustina explains that some crimes would only have been committed if the Internet had these elements. An example is the anonymity of the Internet, many individuals hide behind fake profiles or IP addresses to commit crimes such as cyberbullying, or sextortion. [89] As introduced in Chapter 1, cryptocurrencies' actual characteristics of decentralization and anonymity attract criminals to use them to commit or facilitate illicit activities.

The lack of centralization implies that no third parties are involved in the economic relationships governed by cryptocurrencies. [90] Therefore, there are no external control or rules governing how the relationships between the parties to a transaction should be, nor between the user and cryptocurrencies. This implies a financial system that completely differs from the conventional one that is usually primarily governed by state actors. Thus, 'official' currencies are under a country's jurisdiction; they must comply with their laws and be subject to their control mechanisms and enforcement institutions. [91] Subsequently, decentralization implies the lack of:

1. Crypto- regulations to be governed by.

In this sense, it is essential to clarify that when this thesis emphasizes the absence of regulation, it refers primarily to instruments for controlling the relationship between users and cryptocurrencies. For instance, guidelines and rules widely used in the financial business, such as know your customer standards (which requires that everyone who opens an account must identify itself, while the company must corroborate the identity given). With the imposition of these rules, as occurs with cryptocurrencies, it is possible to

[88] Dr Ramón José Agustina Sanllehí, 'La arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual' [2009] 3(1988-7949) International E Journal of Criminal Science <https://repositori.uic.es/bitstream/handle/20.500.12328/2990/Agustina%20Sanllehi%2c%20Jose%20Ramon_Arquitectura%20Digital%20Internet_2009.pdf?sequence=1&isAllowed=y> accessed 3 March 2023
[89] Ibid
[90] Lee(41)
[91] Rotsay Rosales, 'Poder Política y Democracia' Serie de Cuadernos Didácticos: Teoría y Práctica de la Democracia (Instituto Interamericano de Derechos Humanos, 2012)

understand the nature of customer activity, qualify whether the source of funds is legitimate, and identify the real customer if his financial activity is unlawful. [92]

2. Authorities to enforce such laws and prosecute crimes.

As a matter of illustration, if cryptocurrencies are not considered to be legal tender or a means of payment, and someone is the victim of a crypto-related fraud or scam, unlike current banks, which have systems for recovery of money or reversal of transactions, cryptocurrencies lack such institutions and mechanisms of control. [93] The same applies to money laundering or terrorist financing. Crimes are not prosecuted by leaving out a third party in the transactions. The reason is that there are no intermediaries to control the transactions and detect the presence of suspicious financial movements. [94] If these activities are not detected, they are not prosecuted. In cases of financing of terrorism and money laundering, it can lead to hazards to the socioeconomic order of a country, or in the case of terrorism, endanger the national security of another. [95] [96]

3. Institutions to provide cryptocurrency users with the relevant mechanisms to protect their rights.

As a consequence of the two previous aspects, if a crime is not prosecuted, it is impossible to compensate the victims for the damage caused. The same applies if there is no institution to back the transactions up, as in the case of banks and fraud insurance.

All these motives make decentralization attractive to criminals. Therefore, they choose these technologies to perpetrate an offense, as they make the prosecution of a crime and the identification of the criminal more difficult.

---

[92] Shufti Pro, 'KYC Guide UK' (2021) https://shuftipro.com/reports-whitepapers/KYC-guide-UK.pdf> accessed 3 March 2023

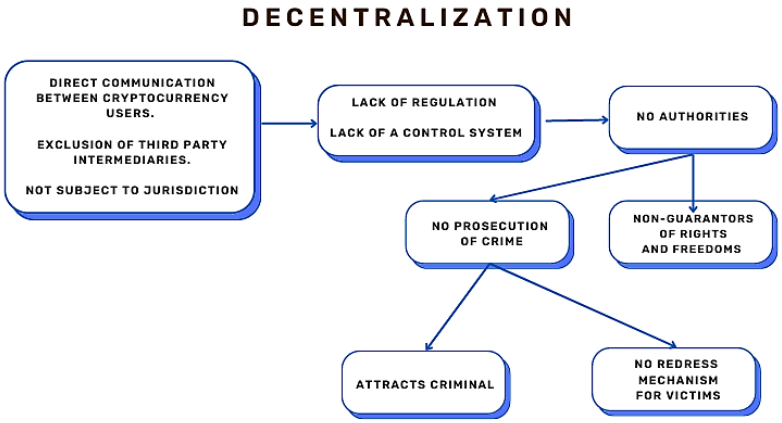
[93] Congressional Research Service, 'Cryptocurrency: The Economics of Money and Selected Policy Issues' (April, 2020) https://sgp.fas.org/crs/misc/R45427.pdf> accessed 3 March 2023

[94] Covadonga Mallada, 'La financiación del terrorismo desde la perspectiva de las nuevas tecnologías A propósito de la quinta Directiva de la UE de prevención del blanqueo de capitales y la financiación del terrorismo' [2018] 71(1) Universidad de Valladolid

[95] Michael Barr and others, 'Enhancing anti-money laundering and financial access: Can new technology achieve both?' [2018] 1(1) The Brookings Institution <https://www.brookings.edu/wp-content/uploads/2018/04/es_20180413_fintech_access.pdf> accessed 10 March 2023

[96] Office of the United Nations High Commissioner for Human Rights, 'Human Rights, Terrorism and Counterterrorism´ (n.d) Https://www.ohchr.org/sites/default/files/Documents/Publications/Factsheet32EN.pdf> accessed 10 March 2023

Illustration 3: Decentralization Outline [97]



Concerning anonymity, it is important to recall what was discussed in Chapter 1. Thus, even though transactions are public, the parties to such a transaction are not. This is not indicative that the wallets of the sender and receiver of the money cannot be traced in any way. Therefore, a real identity doesn't need to be associated with a certain wallet. Thus, anyone can fabricate an identity or use a stolen one. [98]

Furthermore, due to this anonymity, there are no history records associated with specific persons or entities. In a nutshell, the transactions neither require nor provide identification and verification of actual participants. As Dr. Agustina claimed in his paper, anonymity gives a sense of impunity. [99] This feeling is the one that leads to utilize these technologies as illegal means. [100]

Finally, one of the features of cryptocurrencies that are less often mentioned as a potential criminal element is the speed of the blockchain in carrying out transactions. Cryptocurrencies' fast payments engage in illicit activities, mainly money laundering and financing of terrorism, as they are capable of avoiding control and prevention

[97] Source: Claudia Germán [diagram of] 'An outline of how decentralization works', based on [Footnotes from 79 to 83] (30 March 2023)
[98] M Harrigan, 'An Analysis of Anonymity in the Bitcoin System' [2012] 3(1) 11Clique Research Cluster, Complex & Adaptive Systems Laboratory, University College Dublin, Ireland <10.1109/PASSAT/SocialCom.2011.79> accessed 7 June 2022
[99] Agustina Sanllehí (82)
[100] M Möser, 'Anonymity of Bitcoin Transactions an Analysis of Mixing Services' (*University of Münster*, 2013) <https://www.wi.unimuenster.de/sites/wi/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf> accessed 7 June 2022

mechanisms. For instance, they manage to circumvent the tools for detecting suspicious transactions. [101]

2.4 Conclusion

Cryptocurrencies are a peer-to-peer version of electronic money. They work through blockchain technology, which uses algorithms. Besides describing how cryptocurrencies work, this chapter has explained their criminogenic potential, which can be summarized as follows:

- The speed of transactions circumvents the control mechanisms that seek to prevent certain crimes, such as money laundering.
- The anonymity gives a sense of impunity, which encourages criminals to adopt cryptocurrencies without being caught by the authorities.
- And decentralization prevents any institution, safeguard, or guarantor from exercising control over cryptocurrency activities.

Having set out the criminogenic potential of cryptocurrencies, and their implications, the first sub-question of this thesis has been answered, therefore the focus should be shifted to the regulatory approaches of China and the European Union.

Chapter 3. Regulatory approaches to tackle the criminogenic potential of cryptocurrencies: The European Union. (EU)

Cryptocurrency regulation in the European Union has been an evolving topic and has gone through several phases over the years. Indeed, their regulation has been a slow process, and even today new proposals for their legislation are being considered. [102] Unlike the regulation of other technologies such as Artificial Intelligence where the European Union has conducted a more aggressive approach, cryptocurrencies have

[101] Committee on payments and market infrastructure, 'Fast payments: Enhancing the speed and availability of retail payments' [2016] 1(ISBN 978-92-9259-003-1) Bank for International Settlements <https://www.bis.org/cpmi/publ/d154.pdf> accessed 10 March 2023

[102] For instance, a regulation for tracing transfers of crypto – assets has been discussed in the European Parliament on April 2023. Eu parliament, 'Crypto-assets: green light to new rules for tracing transfers in the EU' (*News European Parliament* , April 20 2023) <https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu> accessed 5 May 2023

lacked a harmonized regulation at the European level.[103] The EU regulatory approach regarding cryptocurrencies is divided into two levels: Union and Member State Level (MS). The following sections explore the most significant European Union crypto regulation regarding the illicit use of cryptocurrencies.

3.1 Regulatory Background: The European Court of Justice's Ruling: *Skatteverket v David Hedqvist* [104]

The ruling of the Fifth Chamber in Case C-264/14 *Skatteverket v David Hedqvist,* in 2015 (Case C-264/14) is considered the most relevant case law regarding the regulation of cryptocurrencies because the EUs regulatory approach is built on this ruling. Up to this ruling, the EU had been incapable of reaching a consensus on the legal framework to which crypto assets had to be subjected.[105] Furthermore, this ruling was crucial to include cryptocurrencies within the material scope of several existing regulations.

As it was not established whether cryptocurrencies were considered under the same regime as fiat money or if they constituted a new form of payment, the discussion regarding their consideration in the market and their possible regulation perpetuated the lack of legal framework in which to set them. [106] This decision issued by the ECJ entailed two significant consequences. Firstly, the ruling became a judicial precedent and consolidated the taxation regime of crypto assets. Secondly, it clarified the consideration cryptocurrencies had to have within the European Union's jurisdiction and the regulations that could apply to them. [107] Regarding the pleas of fact, Mr. Hedqvist wanted to provide,

---

[103] Kamil Winnowicz, Cam-Duc Au and Dirk Stein, 'Regulation of Cryptocurrencies in the European Union – Impact of the European Regulatory Notifications on the cryptocurrency market' (4th International Conference on Applied Research in Business, Management and Economics, Prague, 2022) < https://www.researchgate.net/publication/359391758_Regulation_of_Cryptocurrencies_in_the_European_Union_-Impact_of_European_regulatory_notifications_on_the_cryptocurrency_market > Accessed 27 August 2022

[104] Judgment of the Court (Fifth Chamber) of 22 October 2015 Skatteverket v David Hedqvist Request for a preliminary ruling from the Högsta förvaltningsdomstolen Reference for a preliminary ruling — Common system of value added tax (VAT) — Directive 2006/112/EC — Articles 2(1)(c) and 135(1)(d) to (f) — Services for consideration — Transactions to exchange the 'bitcoin' virtual currency for traditional currencies — Exemption
Case C-264/14 https://curia.europa.eu/juris/liste.jsf?num=C-264/14

[105] Kamil Winnowicz, Cam-Duc Au and Dirk Stein, 'Regulation of Cryptocurrencies in the European Union – Impact of the European Regulatory Notifications on the cryptocurrency market' (4th International Conference on Applied Research in Business, Management and Economics, Prague, 2022) < https://www.researchgate.net/publication/359391758_Regulation_of_Cryptocurrencies_in_the_European_Union_-Impact_of_European_regulatory_notifications_on_the_cryptocurrency_market > Accessed 27 August 2022

[106] Ibid

[107] Case C-264/14, Skatteverket v. David Hedqvist, 2015, INFOCURIA – CASE-LAW OF THE COURT OF JUSTICE (Oct. 22, 2015) (ECJ Preliminary Ruling).

through a company located in Sweden, services for the exchange of traditional currencies for Bitcoin. Transactions were to be conducted electronically via the website. Thus, Bitcoin would be acquired directly from companies, individuals, and international exchanges and then sold to those who placed orders with the company.[108] In this context, the Supreme Administrative Court referred two questions to the ECJ for a preliminary ruling:

1. Whether or not the activity carried out by Mr. Hedqvist fell under the scope of Directive 2006/112/EC *on the standard value-added tax.* Therefore, if as any other currency, whether it was subject to VAT or not.

2. If, subject to VAT, whether or not such activity would be exempt or not based on article 135.1 of the Directive mentioned above. [109]

Regarding the first question, the ECJ ruled in the affirmative, concluding that cryptocurrency exchange transactions are subject to VAT. The rationale is that these currencies cannot be qualified as tangible goods according to Article 14 of the VAT Directive, since their sole purpose is to function as a means of payment. [110] In addition, the ECJ determined that the exchanges of different payment methods did not involve the submission of goods; according to Article 24 of the Directive, they had to classify as a service based on Article 24 of the VAT Directive. Likewise, the ECJ confirms the onerous nature of these transactions, proving the existence of a direct relationship between the service provided and the consideration received by the taxable person.

Concerning the second question, once the VAT liability was resolved, the ECJ had remained to determine whether the exemption for financial transactions provided in Article 135.1.d to f of the VAT Directive were applied to the transactions in question, and consequently, whether they are or not exempt from VAT. [111] The ECJ also ruled in the affirmative on its exemption. The Court determined that the transactions exempt from VAT are, by nature, financial transactions without it being necessary for them to be carried out by financial institutions. Furthermore, the Court considered applicable to cryptocurrencies the exemption provided in Article 135.1.e) of the VAT Directive, according to which MS shall be exempt from VAT transactions involving currency,

[108] Ibid
[109] Ibid
[110] Ibid
[111] Ibid

banknotes, and coins which are lawful means of payment. [112] Synthesizing the most relevant ideas to Case C-264/14 [113] :

Firstly, a bidirectional flow of virtual currency like Bitcoin and other crypto assets, which is exchanged for traditional currencies in an exchange transaction, cannot be considered tangible because its sole purpose is to serve a payment. As any other supplies of services of an onerous nature in the territory of a MS by a taxable person, cryptocurrencies are subject to VAT (ex. art. 2.1 VAT Directive). The ECJ applied the principle of equal treatment, implying that although cryptocurrencies are not legally protected, due to their function as legal means of payment, then, it could be stated that they are services rendered in exchange for a consideration that is related to those services rendered. Secondly, only exemption applicable to cryptocurrencies is the one typified in article 135.1.e. Case C-264/14 has created a landmark in crypto regulation. Firstly, the ECJ has become the first court to discuss the legal aspect of cryptocurrencies and its tax system, which has created a forum of controversial opinions among scholars. Some consider this court ruling erroneous because it concludes that cryptocurrencies are a payment method like traditional currencies. This equating among currencies is the origin of the error and controversy. For some scholars, such as González, these currencies serve more as an investment mechanism rather than a means of payment. [114] On that account, cryptocurrencies should not be considered '*general methods of payment'* since i.) it always requires express admission of both parties and ii.) '*legal means of payment'* in Article 135 VAT Directive refers solely to currencies issued in a regulated market and backed by international bodies. According to the author, the ECJ should have considered cryptocurrencies as mere '*means of exchange'. [115]* Moreover, the author criticizes that the ECJ in this ruling appears to be a promoter of the use of privately established digital currencies. These alternative means of payment are neither legally established as currencies, nor are they legal tender issued by central banks and other public authorities, as previously mentioned.

On the contrary, other authors have found this ruling groundbreaking. The ECJ ruling has been envisioned as a step forward in adopting a cryptocurrency regulation. The ruling

[112] Ibid

[114] Gónzalez Marta, ' Fiscalidad aplicable a los bitcoines a la luz del ordenamiento tributario español' (AEDAF Revista Técnica Tributaria, 2017)
[115] Winnowicz(100)

refuses to interpret cryptocurrencies in the traditional form and opts to apply the existing law and principles in a more flexible form. Therefore, it is in line with technological development. Scholar Daniel Lyons states this ruling '*may boost confidence in cryptocurrencies and could lead to a wider adoption'.* [116] This is an exact conclusion, considering the ruling of the ECJ mentions the possibility of creating a harmonized crypto regulation given its future expansion. Indeed, the court advocates for a '*smart regulation to foster innovation and ensure integrity.'* In short, the ECJ calls for a proportionate regulatory approach at the Union Level while considering the challenges it may pose in regulating the widespread use of currencies. [117]

This claim brings us to the second rationale for why this ruling is crucial: the ruling is binding for all MS In the absence of a European standard that established a common criterion, some MS (e.g., Poland) were taxing Bitcoin, while other MS (such as Portugal) did not. Following this decision, all MS must apply for the VAT exemption, thus becoming a harmonized regulation. Furthermore, the ECJ identifies in the ruling the laws directly applicable to blockchain technologies and cryptocurrencies, establishing them as sufficient regulatory frameworks regardless of the underlying technology.[118] Briefly, the ECJ considers that:

- All cryptocurrencies are excluded from the regulation under regulation Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 *'on the taking up and pursuit of the business of electronic money institutions.*

[116] Daniels Lyons, 'European Court of Justice rules that Bitcoin should be treated as a currency for VAT purposes' (*Deloitte*, 22 October 2015) <https://www2.deloitte.com/uk/en/pages/press-releases/articles/european-court-rules-bitcoin-be-treated-as-currency-for-vat.html> accessed 7 November 2022.

[117] Winnowicz (100)

[118] Therefore, cryptocurrencies are encompassed in the following laws: i.) Regulation (EU) No 648/2012 of the European Parliament and the Council of 4 July 2012 on OTC derivatives, central counterparties, and trade repositories. ii.) Regulation (EU) 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and central securities depositories; iii.) Directive (EU) 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and central securities depositories; iv.) Directive (EU) 98/26/EC of the European Parliament and of the Council of 19 May 1998, on settlement finality in payment and securities settlement systems; iv.) Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems; v.) Regulation (EU) 600/2014 of the European Parliament and of the Council of 15 May 2014, on markets in financial instruments; vi.) Directive (EU) 2014/91/EU of the European Parliament and of the Council of 23 May 2014 on markets in financial instruments; and European Parliament and of the Council of 23 July 2014 amending Directive 2009/65/EC on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities and vii) Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers.

The reason is that the ECJ dismisses the qualification of cryptocurrencies as electronic money (Art 14 VAT Directive).

- Cryptocurrencies are excluded from the regulation of markets in financial instruments and investment services (MiFID Directives). The reason given by the ECJ is that cryptocurrencies are not considered a derivative.
- The ECJ recommends including cryptocurrencies under the Anti-Money Laundering Directive. [119]

In summary, this ruling represents a turning point in the EU´s regulatory approach of cryptocurrencies as it consolidates the legality of cryptocurrencies within its jurisdictions and provides legal certainty regarding applicable laws and the material scope under which cryptocurrencies can be categorized.

3.2 The 5th Anti-Money Laundering Directive (5AMLD). [120]

This Directive arose as a consequence of the increasing cooperation between terrorist and criminal groups, which led to the need to adopt more efficient measures relating to the prevention and prosecution of the commission of crimes involving *inter alia,* money laundering, and terrorist financing.[121] Following the worldwide switch to virtual money and the impact this had on money laundering and terrorism financing, the EU amended its regulation to keep up with the digital era's challenges. [122] This Directive is worth exploring because, along with the ruling of the Fifth Chamber in Case C-264/14 *Skatteverket v David Hedqvist,* in 2015, the 5ADML is considered by European Authorities as one of the first steps the European Union took with the unique purpose of regulating cryptocurrencies. [123]

---

[120] The 5AMLD refers to Directive (EU) 2018/843 of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU.[120]

[121] Kenton W, "Anti Money Laundering (AML) Definition: Its History and How It Works" (InvestopediaAugust 29, 2022) <https://www.investopedia.com/terms/a/aml.asp> accessed December 2, 2022

[122] "EU Context of Anti-Money Laundering and Countering the Financing of Terrorism" (*Finance*) <https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en> accessed December 2, 2022

[123] News European Parliament , ' Crypto-assets: green light to new rules for tracing transfers in the EU' (*News European Parliament* , 20 April 2023) <https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu> accessed 16 May 2023

Among the objectives the Directive intends to achieve, the European Council and Parliament emphasized:

- Safeguarding the integrity of all the MS financial systems.
- Protecting and ensuring EU citizen's safety.
- Creating a unique and harmonized regulatory framework to mitigate the legislative challenges raised by legal loopholes, the globalization of terrorist organizations, and the emergence of technological innovations. [124]

The Directive's preface emphasizes that it seeks to accomplish the above objectives. It was, therefore, necessary to enact amendments to Directives 2009/138/EC and 2013/36/EU, to broaden their scope to cope with regulatory challenges arising from the emergence of crypto assets and other technologies. Among the various amendments the 5AMLD introduces, it is worth highlighting Article 3. This article shows how the Directive follows the ruling in Case C-264/14, defines virtual currencies, and reaffirms their legal nature as means of payment within the European Union. [125] (Their legal status was not included in the previous Directives). Other novelties the 5AMLD introduces relate to cryptocurrency´s service providers, particularly, regarding the figure of the service providers responsible for the exchange of 'virtual currencies' for 'fiat currencies and those service providers whose primary function incorporates the safeguarding of 'wallets'.[126] Before the enactment of the 5AMLD, cryptocurrency exchanges or service providers did not have any obligation regarding the monitoring and control of cryptocurrencies. For this reason, 5AMLD incorporates cryptocurrency´s service providers as obligated parties in the scope of their actions. The 5AMLD aims to exercise greater control over cryptocurrency transactions being carried out within the European Union and achieve a higher detection and prevention of criminal actions related to money laundering and terrorist financing. Consequently, these cryptocurrency service providers are required to operate within the boundaries of the EU´s law, which will help them combat the decentralized nature of these crypto assets. [127] Another of the aims pursued by

[124] Kenton W (116).
[125] Article 3 Digital currencies are digital representation of value not issued or guaranteed by a central bank or public authority, not necessarily associated with a legally established currency, not possessing the legal status of money or currency but accepted by natural or legal persons as a medium of exchange, and which can be transferred, stored and which can be transferred, stored and traded by electronic means.
[126] Found in the explanatory memorándum, articles 1 and 45 of the 5AMLD.
[127] As it will be seen in MICA Regulation, it requires registration.

the European Union in its battle for the eradication of money laundering and the financing of terrorism is to achieve greater transparency in the financial sphere since it is a determining factor in both preventing and detecting the commission of criminal offenses. [128]

The 5AMLD has played its part and realized that regulation must tackle the features that make cryptocurrencies both unique and hazardous. Consequently, the 5AMLD has introduced certain amendments to the previous Directive to combat the anonymous nature of crypto assets. For instance, article 13 sub a requires not only have to verify the identity of the users through the integral and autonomous databases, but it must identify all the users who carry out their activities through electronic media. In this way, all the information related to the identity of the various users who perform transactions with cryptocurrencies would be more automated, thereby diminishing the risks associated to anonymity. [129]

In the area of identification, the Directive assigns Financial Intelligence Units (FIUs) a series of competencies MS must respect and enforce. For instance, MS must facilitate access to the FIUs of information identifying natural or legal persons utilizing registers or electronic access systems. Moreover, only national FIUs can obtain any information that allows them to associate the addresses of virtual currencies with the identity of the owner of the virtual currency.[130] The 5AMLD also extends the scope of FIUs by promoting cooperation among jurisdictions, states, and entities. To do so, the Directive requires appropriate cooperation with law enforcement and judicial services to exchange data or information whenever there is a suspicion of a crime, particularly terrorist financing. The information must circulate directly and as quickly, without undue delay or hindrance. [131] Finally, FIUs must be able to obtain from any obliged entity all necessary information related to their functions so they can ensure the tracing of capital flows and the early detection of illicit networks and flows.[132]

Furthermore, this Directive increases the level of enhanced due diligence. This way, service providers have a series of duties, from the prohibition of anonymous bank

[128] Niels Vandezande, 'Virtual currencies under EU anti-money laundering law' [2017] 33(341-353) ELSEVIER
[129] Article 13 AMLD, Ibid. (113)
[130] Article 17 AMLD
[131] Kenton W116)
[132] Kenton W (116)

accounts (Art 10) or stricter *know your costumer (KYC)* measures (Art 14). [133] Enhanced due diligence will also be required when the transactions involve a high-risk country or are illogical from an economic point of view. Indeed, service providers are required to report any suspicious activity. As an indirect consequence of the requirement for the treatment of the customer's data or services, the Directive obligates services providers to act according to the provisions set in the GDPR. Finally, the 5AMLD states that MSshall impose criminal and administrative sanctions, and that these must be '*effective, proportionate, and dissuasive'*. [134]

3.3 Market in Crypto Assets Regulation: The MiCA Proposal.

In 2020, the European Commission presented the "Digital Finance Package" (DFP) under the claim that it would lead the European Union into the digital age in the coming decades. This package aimed to improve the competitiveness of the sector and Europe's FINTECH technologies while mitigating risks and ensuring the financial stability of the European Union's economy. [135] [136] The DFP contains the Market in Crypto Asset (MiCA) Regulations, which aims to create a regulatory framework for crypto assets. [137]

The MiCA proposal arose in response to the reports published by the EBA and the ESMA regarding the normative status of cryptocurrencies in the European Union.[138] Both reports claimed that most crypto assets fell outside the scope of the EU's legislation, since, in

[133] Articles 10 & 14 5AMLD. Ibid (113)

[134] Sanctionable conducts, refer in essence of the breach of the aforementioned duties of diligence (arts. 59.1 and 59.2) and may be imposed on the obliged entities even when the conduct is attributable to their managers or representatives if it was due to the lack of supervision or control of such entities.

[135] International monetary fund, 'In September 2020, the European Commission presented the "Digital Finance Package" (DFP) under the claim that it would lead the European Union into the digital age in the coming decades This package aimed to improve the competitiveness of the sector and Europe's FINTECH technologies while mitigating risks and ensuring the financial stability of the European Union's economy ' [2022] 22(243) International Monetary Fund <file:///C:/Users/User/Downloads/1IRLEA2022009.pdf> accessed 17 May 2023

[136] Werner Vermaak, 'MiCA (Updated July 2022): A Guide to the EU's Proposed Markets in Crypto-Assets Regulation' (*SYGNA*, July 2022) <https://www.sygna.io/blog/what-is-mica-markets-in-crypto-assets-eu-regulation-guide/> accessed 12 November 2022

[137] i.) Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology. ii.) Proposal for a Regulation of the European Parliament of the Council on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (known as the Resilience Proposal or DORA); iii.) Proposal for a Regulation of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/234. iv.) Proposal for a Regulation of the European Parliament and of the Council on crypto-asset markets and amending Directive (EU) 2019/1937 known as MiCA proposal.

[138] Financial Stability Board, 2022, 'Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets.' (FBS, October 2022) https://www.fsb.org/wp-content/uploads/P111022-3.pdf

accordance with the ruling of Case C-264/14, cryptocurrencies are not subject to the MiFID Directives). This regulatory gap implied that crypto customers and investors found themselves vulnerable to the risks associated with using cryptocurrencies, such as investment fraud.

The MiCA regulatory proposal is characterized by placing the consumer at the forefront of its protective scope. Along with its core aimsproviding legal certaintysecuring the market integrity; and embracing innovation; to ensure the protection of the crypto consumers is set in the Preamble as the cornerstone goal of the proposal. [139]

In order to ensure the rights of crypto users the MiCA has put forward a series of procedural and conduct rules for the issuers and the service providers of the crypto assets. With the new rules, both actors must comply with strict requirements. For instance, article 53 requires that crypto assets can only be provided or issued by legal entities whose registered office is in a MS of the EU. [140] In addition, a license is required to function as a crypto-asset service provider or issuer, for which an application for authorization must be filed with the authorities where the legal entity has its registered office.

Chapter 2 of Title V explicitly addresses the obligations applicable to all crypto-asset service providers (CASP). Article 59 imposes the obligation to act honestly, fairly, and professionally in the best interest of their clients. [141] This precept specifies that crypto-asset service providers shall provide their customers with fair, transparent, and non-misleading information. Likewise, it states that they must not deliberately or negligently mislead customers concerning the actual or perceived advantages of crypto assets. It must warn of the risks associated with the purchase of crypto assets. CASP will be held liable in case they lose investors' crypto assets. Indeed, article 13.2 establishes that when cancellation of the issuance occurs, service providers must return the buyer's funds raised.[142] The MiCA requires rigorous compliance of security protocols for further consumer protection. Regarding personal data, article 88 of the MiCA proposal demands compliance with the GDPR. For instance, when the travel rule requires data, but data

[139] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937
[140] Article 53 MICA Proposal Ibid (129)
[141] Article 59 MICA Proposal Ibid (129)
[142] Article 13.2 MICA Proposal Ibid (129)

protection is not guaranteed, the MiCA establishes that such data shall not be sent. Along the obligations required by the MiCA proposal there is:

- A proposal for issuers and service providers to follow effective security protocols in accordance with the European Union standards.
- A proposal for issuers and CASP to follow the guidelines published by the ESMA and the EBA. Therefore, the European Union achieves unified standards. [143]

These regulatory proposals provide certainty to the consumer when interacting with cryptocurrencies. Through the control and identification of issuers and providers, as well as their legal domicile, the characteristics of their cryptocurrencies, limitation of assets that can be issued, the EU, on the one hand, intends to control cryptocurrencies within its jurisdiction. Furthermore, through security and conduct protocols, as well as the establishment of liability of issuers and CASP, consumers are provided with greater protection, not only within the business relationship but against the potential offenses that emanate from cryptocurrencies in the market. [144]An example strongly associated with the MiCA proposal is to mitigate fraud schemes, investment scams, or fake exchanges of currencies.[145]

Furthermore, it is noteworthy to explore the MiCA proposal regarding money laundering and terrorist financing crimes. The proposal does not directly tackle the challenges of terrorist financing and money laundering. Indeed, the MiCA derives this responsibility to the regulations that have already been enacted in these matters, e.g.: the 5thAMLD. Thus, the MiCA designates itself as a complementary tool. Nonetheless, in consideration 8 of the Draft, the European Commission clarifies that: *'while the purpose of this Regulation is not to address anti-money laundering and combatting issues raised by crypto-assets, this Regulation should contribute to this objective.'* [146] Moreover, the proposal showcases its intention to comply with the recommendations published by the Financial Action Task Force.[147] For instance, the proposal in consideration 53.a.) requires that authorized CAPS

[143] Ibid.
[144] Ibid
[145] Financial Stability Board (132)
[146] Financial Stability Board Consideration 8 MICA Proposal Ibid (132)
[147] The Financial Action Task Force is an international policy-making and standard setting body dedicated to combat money laundering and terrorist financing. It was created by the G-7 in 1989 in response to a growing concern about money laundering. Us department of the treasury , 'Financial Action Task Force' (*US DEPARMENT OF THE TREASURY* , Unknown) <https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/financial-action-task-

in the European Union apply enhanced scrutiny of financial transactions with customers and financial institutions from third countries included in the list of high-risk countries, which have strategic weaknesses in their anti-money laundering and counter-terrorist financing regimes. [148]

The European Parliament presented a 2020 report on MiCA. The report proposed that after the entry into force of the regulation and after consulting the EBA and ESMA, the European Commission must present a periodical report that includes an assessment of the level of threat of terrorist financing, money laundering, and other offenses related to cryptocurrencies regarding the usage of the decentralized financial system. Therefore, the EU can implement the necessary measures and sanctions aiming to prevent illicit activity regarding the transaction of crypto-assets. [149]

3.4 Member States' Regulatory Approach

Akin to many other technologies, cryptocurrencies are not limited to a specific jurisdiction, as its operation and impact are transnational. This borderless nature entails a regulatory challenge since the potentially harmful effects of these technologies are also detached from territorial boundaries. The ability of cryptocurrencies to enhance the commission of crimes on a multi-level scale is what has led global powers such as Europe to highlight the need for harmonized regulation, and the cooperation of all the international players. However, this need seems to be difficult to accomplish, as the EU still lacks a harmonized regulatory framework regarding cryptocurrencies. [150] Thus, has resulted in legal loopholes and inconclusive regulations at the EU level. Consequently, some MS have considered enacting national legislation on a subsidiary form to better regulate crypto.

Spain has been an example of this. Although it has taken a very prudent approach when regulating crypto, legislators have included cryptocurrencies under the scope of several national laws. It must be noted that Spanish authorities (such as the Government or the

force#:~:text=The%20Financial%20Action%20Task%20Force,money%20laundering%20and%20terrorist%20financing.> accessed 24 March 2023

[148] Consideration 53.a.) MICA Proposal Ibid (133)

[149] ESMA, Advice on 'Initial Coin Offerings and Crypto-Assets', 2019; EBA report with advice on cryptoassets, 2019. 17 https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[150] García Gabilondo M, 'Regulación de los criptoactivos. Análisis del régimen jurídico propuesto en la UE para los activos digitales y del régimen aplicable a los DTL Tokens.' (Degree Final Dissertion, Universidad de Comillas, 2021)

Central Bank of Spain) consider crucial that the EU takes the lead in regulating cryptocurrencies as this phenomenon has a transnational nature. [151] Indeed, these institutions have reminded legislators of the hazards these assets pose to the country.[152]

In the case of Spain, the dissonance was to be found in social behavior rather than in political discourse. Spain has consolidated its position as the fifth country in Europe with the highest number of transactions made with cryptocurrencies.[153] The Bank of Spain made a report concluding that 1 in 10 Spanish adults owns a crypto asset. Since their hype, cryptocurrencies have rapidly spread and taken root in Spanish society.[154] This popularity of cryptocurrencies is also taking its toll on Spanish criminal law, which has seen crime rates rise in two crimes: money laundering and fraud. [155] Here is where the Spanish regulatory position is worth mentioning. Any legal system faced with a new phenomenon that jeopardizes and damages its core interests – e.g., legal functioning of the economic and financial system, the protection of the administration, national security, in cases of money laundering and terrorist financing – would create a series of regulatory mechanisms to protect those interests. For instance, in the case of fraud, in the year 2022, it is estimated that 17,000 Spaniards have become victims of a worldwide cryptocurrency fraud. [156] [157] Most cases of fraud in Spain in this area relate to investments. Many investment frauds have resulted from fraudulent campaigns with celebrities such as Lionel Messi at the forefront, giving citizens without financial knowledge a sense of security to invest.[158]

---

[151] "Blockchain & Cryptocurrency Laws and Regulations: Spain: GLI" (GLI - Global Legal Insights - International legal business solutions) < https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/spain> accessed November 12, 2022 Indiem, 'Marco normativo de las criptomonedas en España ' (*Indiem Abogados*, April 10 2023) <https://www.in-diem.com/abogados/criptomonedas/criptomonedas-regulacion-legal-espana-y-comparada> accessed 22 May 2023

[152] García Gabilondo M (143, 144)

[153] Martínez J, "España Es El Quinto País De Europa Con Mayor Volumen De Transacciones En Criptomonedas" (*BeInCrypto*April 27, 2022) <https://es.beincrypto.com/espana-quinto-pais-europa-mayor-volumen-transacciones-criptomonedas/> accessed December 2, 2022

[154] Marca, "Uno De Cada Diez Espa" (*MARCA*September 17, 2018) <https://www.marca.com/tecnologia/2018/09/17/5b9fbdefe5fdea00498b4643.html> accessed November 14, 2022

[155] IP Specialist (69)

[156] In this case, criminals posed as brokers and advised people to invest hundreds of thousands of euros in Bitcoin. Then, once they had the money, criminals fled with it.

[157] MAYKA NAVARRO 14/11/2022 14:39Actualizado a 14/11/2022 18:50, Navarro M and Getty, "Más De 17.000 Víctimas En España Arruinadas En Una Estafa Mundial Con Criptomonedas" (*La Vanguardia*November 14, 2022) <https://www.lavanguardia.com/vida/20221114/8606408/desmantelada-red-criminal-criptomonedas-17-000-victimas-espana.html> accessed December 2, 2022

[158] "Famosos En Los Anuncios De Las 'Cripto'" (Expansion) < https://www.expansion.com/blogs/peon-de-dama/2022/01/23/famosos-en-los-anuncios-de-las-cripto.html> accessed November 16, 2022

Spain has responded to the crime of fraud in two ways:

1. The National Securities Market Commission (CNMV) issued Circular 2/2020, dated October 28, of the National Securities Market Commission, on the advertising of investment products and services, by which massive advertising campaigns are regulated both in traditional media and in social networks, which, in context, are aimed at 100,000 people or more. Although this regulation will not apply uniquely to crypto assets themselves, the agency has clarified that it included under its material scope that all advertising related to Bitcoin, or any other cryptocurrency must warn investors about the risks of these products. The new regulation only indicates the requirements to be met by advertising activity offering crypto assets as possible investment instruments. Likewise, the CNMV informed that this new rule defines how the agency will supervise all advertising material and establishes a mandatory prior communication regime for massive campaigns.[159]

2. To penalize the crime of fraud through the Penal Code, where this crime is already typified under art. 248 et seq. In 2019, the Spanish Supreme Court ruled for the first-time regarding cryptocurrencies in relationship to a continuing offense of fraud and misappropriation. A company, Cloud Trading & Devs LTD undertook to manage the bitcoins of 'M, S Ó, Y, and J' (in the ruling), having to re-sell them, and to submit at the expiration of the contract the profits obtained, in exchange for a commission.[160] The court, without going into definitions of the cryptocurrency, or the technology used, ruled the company for fraud to two years in prison and the return of what was swindled in euros from the bitcoins at the time the fraud was consummated. [161]

This national position is particularly interesting. In the face of their difficulty to specifically regulate cryptocurrencies and delegate them to the European Union, Spain has been able to interpret their rules in a more flexible manner, including cryptocurrencies under their legal mantle. It does not encounter the regulatory difficulties the European Union seems to face. Perhaps this is the approach Europe should adopt. In the face of the

[159] Gómez Rodríguez C, 'Las criptomonedas y su regulación penal: Normativa antiblanqueo', (Degree Final Dissertation Universidad de Comillas, 20222).
[160] Roj: STS 2109/2019 – ECLI: ES:TS: 2019:2109. Id Cendoj: 28079120012019100389 Órgano: Tribunal Supremo. Sala de lo Penal Sede: Madrid
[161] Ibid

'regulatory vacuum' due to the lack of rules governing cryptocurrencies, Spain made up for it with the laws in force. Even in criminal matters, the MS clarify that cryptocurrencies are not a problem for prosecution and imprisonment since they are just another means to commit a criminal act. Finally, to conclude that the position of the States to regulate and prosecute crimes in a subsidiary manner can be effective, and the European Union should mimic it.

3.5 Conclusion

From the laws analyzed, we can observe that the European Union takes several measures to combat the potential for crime. The ECJ ruling not only establishes the legal status of cryptocurrencies within the European Union but also provides a harmonized definition that allows them to be defined singly. This means that there are no legislative differences in their treatment within the EU. Likewise, the ECJ ruling is important since it clarifies the legal framework for cryptocurrencies. It also outlines this criminogenic potential by suggesting its inclusion in the 5AMLD. On the other hand, the 5AMLD also includes in its scope the fight against terrorism, so it is not only limited to money laundering measures. This law includes under its material scope cryptocurrencies, and exchange services or services that provide cryptocurrencies and focuses on decentralization, anonymity, and the transnational aspect of cryptocurrencies. Therefore, it implements measures of customer identification, monitoring, and international cooperation. It even creates special units for the prevention and arrest of these crimes. It adds third-party intermediaries that put an end to decentralization, since transactions are controlled, there is a record of users, quantities, etc. It also puts an end to anonymity, since these cryptocurrency providers or exchanges are required to identify their clients, their purposes, etc. Thus, making it difficult for transactions to be made without knowing the sender or the receiver. Finally, the MiCA proposal is another measure aimed at preventing crimes such as fraud, by requiring that all cryptocurrency services that are intended for the public must be registered or licensed, thus preventing fraudulent investment companies from stealing money. This law also puts the focus back on the importance of these establishments acting diligently, assessing potential crimes that may arise in this context. The European Union's regulatory approach to criminogenic potential is one of prevention and action. The legislator is aware of the characteristics that make this technology attractive to criminals and tries to hinder them.

Chapter 4. Regulatory approaches to tackle the criminogenic potential of cryptocurrencies: China.

4.1 Background and Legal Status: The cryptocurrency ban in China.

As in the previous chapter, before delving into the regulation of cryptocurrencies and their criminal use, it is important to understand the context in which these legislations are developed. In the case of China, the relationship between the country and cryptocurrencies is complex and replete with lights and shadows. As previously revealed, cryptocurrencies are banned in the country, but this restrictive stance was not the one adopted by China at first. The legal history of cryptocurrencies in the country has been a cycle of tolerance, prohibitions, and repression.

At first, like the European Union, when cryptocurrencies emerged in 2008, they were an unknown technology to society and lawmakers. Nonetheless, in contrast to the lack of initial attention given to cryptocurrencies in the European Union, they promptly began to become a wildly popular phenomenon in the Republic of China. Proof of this is that in early 2010, China became the country where most Bitcoin transactions took place and most of the cryptocurrency exchanges were located. [162] Further instances that support this allegation of the extremely close relationship that existed between cryptocurrencies and China are that in 2011, the first Bitcoin exchange opened in the country. [163]

By 2014, China had already started mining cryptocurrencies and included this activity within the scope of their industry, and, by 2019, China had established itself as the leading cryptocurrency mining country. Indeed, a study by the University of Cambridge found that in 2019 alone, China controlled 65% of the global hash rate. [164] One of the main reasons for this popularity was the fact that Chinese citizens were seeking ways around financial restrictions and government control over international transactions. Moreover, cryptocurrencies were seen as an opportunity to invest in alternative assets that offered the opportunity for greater financial returns. Many Chinese citizens were also interested

[162] Sharma R, 'China's History with Cryptocurrency' (*Investopedia*, 13 July 2022) accessed 16 May 2023

[163] "Methodology" (*CCAF.io*) <https://ccaf.io/cbeci/mining_map/methodology> accessed November 22, 2022

[164] Hash-rates refers to the number of computational operations that a miner, or rather a network of miners, can perform to solve the cryptographic puzzles that are necessary to generate new cryptocurrencies.
Because cryptocurrency mining requires vast amounts of computing power, energy consumption is a problem for many countries. Considering China has extremely cheap electricity it is not a problem for the country.

in Investment Coin Offerings (ICOs), which allowed them to invest in new cryptocurrencies before they were even launched, which frequently offered significant returns in a brief period. [165]

Despite this popularity, for a long time, there were no specific regulations for cryptocurrencies in China. It was not until 2013 that the country issued the first legal instrument regarding cryptocurrencies. The PBOC and other governmental agencies published the *'Notice Concerning the Prevention of Risks Associated with Bitcoin.'* The Notice focused primarily on the risks associated with investing in these virtual currencies. First, the Chinese government clarified that cryptocurrencies were not recognized as legal tender but should in any case be considered as a virtual commodity. In the second place, the PBOC warned that cryptocurrencies were susceptible to being used for illicit activities such as money laundering or terrorist financing. It also noted that considering that cryptocurrencies were not considered legal tender, companies offering cryptocurrency-related services were not regulated by the Chinese financial authority, which increased the risk of fraud. Thirdly, the PBOC remarked on the excessive speculation in virtual currencies, which could lead to speculative investments and financial losses. Although this warning was focused on alerting Chinese citizens to be cautious when investing in cryptocurrencies, it did not result in a prohibition on their use for the public. The most restrictive aspect of this Notice lay in the financial institutions and banks, which were prohibited from cryptocurrency transactions. Likewise, it was required that exchange houses must register with the government's Telecommunications Regulatory Agency and comply with anti-money laundering (AML) and know-your-customer (KYC) measures. [166]

[165] ICOs are a widely used way for a vast number of start-ups by a vast number of start-ups in the cryptocurrency space to raise capital for their projects. This process consists of a kind of crowdfunding by which a given project attempts to raise funds in exchange for tokens or units of a cryptocurrency generated by the creators of the project in question. Users who decide to participate in these ICOs do so with the expectation that if the project goes ahead those tokens or coins can be re-valued enormously, thus obtaining great benefits.

[166] Due to the difficulty of finding sources in Spanish/English, this fragment contains information from the following sources:
Xie Rain, 'Why China had t Por qué China tuvo que "prohibir" las criptodivisas pero EEUU no: A ency but the US did not: A Comparative Analysis of Regulations on Cr e Analysis of Regulations on Crypto-Markets Between ets Between the US and China ' [2019] 18(2) Washington University Global Studies Law Review.
Comply advantage, 'Is Cryptocurrency Legal in China?' (*Comply Advantage* , 5 July 2022) <https://complyadvantage.com/insights/crypto-regulations/cryptocurrency-regulations-china/> accessed 16 May 2023

From 2013 to 2017, cryptocurrencies were not subject to specific regulations in China. It is important to consider that at that time the legal implications of cryptocurrencies were not yet well understood. Furthermore, China was grappling with several economic challenges, therefore regulating cryptocurrencies was not an immediate priority for the Chinese government at the time. Nonetheless, as the popularity of cryptocurrencies continued to rise, and more cases of cryptocurrency-related fraud and money laundering emerged, China started to gradually ban cryptocurrencies through diverse legislative instruments.

In 2017, seven relevant state agencies published an '*Announcement on the Prevention of Financial Risks of Token Issuance',* prohibiting ICOs, and the exchanging of cryptocurrencies for fiat money or vice versa. [167] The rationale behind the ban was that ICOs began to grow in popularity in the country, and several of them were used to commit fraud. [168] One of the most notorious cases of ICO fraud in China was the OneCoin case. The OneCoin company defrauded around four billion dollars around the world. Hangzhou police suspected that the majority of the money was stolen from Chinese citizens.

Later, in January 2018, China finally banned the use of cryptocurrencies through the publication of a proclamation known as ´The Cryptocurrency Advertising Ban´. In this publishing, China clarified that the country would adopt a '*zero-tolerance policy'* regarding cryptocurrencies, thus restricting all the economic activities related (to mining, and trading). Furthermore, access to foreign cryptocurrency exchange platforms was limited and it ordered the closure of companies offering services related to cryptocurrencies. This constraint was followed by the Chinese Government blocking access to cryptocurrency exchange websites, hosted within the country or abroad. Thus, aiming to complete the total blockade of the cryptocurrency market in the country. [169]

---

[166] Zhou S and Leimin Y, 'Anti Money Laundering Laws and Regulations Report 2022-2023 China' (International Comparative Legal Guides International Business Reports, 2022) accessed 16 May 2023
[166] Ibid.
[167] PBOC, the Central Office for Cyberspace Affairs, the Ministry of Industry and Information Technology, the State Administration for Industry and Commerce of China, the China Banking Regulatory Commission, the China Securities and Exchange Regulatory Commission, and the China Guarantee Regulatory Commission.
Times G, "Over 90% of Crypto-Related Businesses Shut down in China after Ban" (Global Times) < https://www.globaltimes.cn/page/202110/1235801.shtml> accessed December 2, 2022
[168] Michael j Casey , 'It's Political: Why China Hates Bitcoin and Loves the Blockchain' (*Coin Desk* , 27 September 2017) <https://www.coindesk.com/markets/2017/09/27/its-political-why-china-hates-bitcoin-and-loves-the-blockchain/> accessed 3 May 2023
[169] Ibid

China´s last regulatory hurdles concerning cryptocurrencies came in September 2021, when the Chinese government, together with other national authorities published *the `Notice regarding the Rectification of Virtual Currency "Mining" Activities (Fa Gai Yun Xing [2021] No. 1283) (Circular No. 1283)´* by which they finally prohibit the mining of cryptocurrencies, penalized the illegal supply of energy and eliminated all the financial support that had been allocated to it. [170] That same month the PBOC published that it considered all cryptocurrency–business activities as illegal financial activities, including extraterritorial companies that provide online cryptocurrency services to Chinese citizens and residents. [171]

As of today, the prohibition of cryptocurrencies is nearly total, leaving their possession as legal.[172] In 2020 China amended its Civil Code, establishing that cryptocurrencies were a property for purposes of inheritances. [173] China's regulatory approach is extremely restrictive regarding cryptocurrencies. However, although the beginning of the ban took place in 2017-2018, it has been a progressive process, and it is indeed for this reason that the Chinese authorities have continued to enact regulatory instruments aimed at regulating cryptocurrencies.

Many rationales have been attached to the banning process. As explored earlier in this chapter, from the outset, the PBOC argued that these restrictions served security reasons. Firstly, cryptocurrencies were considered a hazard to the Chinese financial system due to cryptocurrency's highly speculative nature. Secondly, because of their criminogenic potential, their inherent potential risks, and the need to protect Chinese citizens from these hazards. Nonetheless, these are not the only reasons that led to the prohibition of cryptocurrencies in the Chinese Republic. Scholars such as Michael Casey and Lucas Lima claim that it is arguable to assume that some other critical reasons made the Chinese government take such a strict measure. [174] For instance, China intended to curb the capital flight or the decentralized nature of cryptocurrencies would have clashed with the

---

[170] The international academy of financial crime litigators and others, 'Working Paper 38: Cryptocurrencies in Asia and Beyond: law, regulation and enforcement ' [2022] Basel Institute on Governance <https://baselgovernance.org/sites/default/files/2022-05/WP-38.pdf> accessed 15 May 2023

[171] Ibid.

[172] China banned all activities related to cryptocurrencies, but their possession remained legal.

[173] Comply advantage, 'Is Cryptocurrency Legal in China?' (*Comply Advantage* , 5 July 2022) <https://complyadvantage.com/insights/crypto-regulations/cryptocurrency-regulations-china/> accessed 16 May 2023

[174] Ibid

Lucas Lima, `Análisis de las criptomonedas en China: Evolución, situación actual y perspectiva´ (Final Degree Project, University of Valladolid, 2022).

centralized political system of the Republic. These two rationales seem logical considering:

1. That according to a Chainalysis publication, around fifty billion dollars' worth of cryptocurrencies flew out of China to other jurisdictions, severely affecting the Chinese economy. [175]

2. That the capital flight was provoking tax base erosion and profit shifting, reducing the country's public revenues. It also reduced domestic market liquidity and lowered asset values. [176]

3. It hindered Beijing's ability to control yuan exchange rates by devaluing the domestic currency. Furthermore, this downward pressure on the yuan led nationals to exchange their coins for stronger foreign currencies (which, as an endless loop, further devalued the yuan). [177]

4. That in 2016 alone, when the yuan devalued due to capital flight, the PBOC had to spend a trillion dollars to stabilize it. [178]

5. That without delving deeper into political matters, cryptocurrencies were challenging the Chinese political system. Considering that the country has an authoritarian political system and a centralized government structure, cryptocurrencies represented a loss of control regarding financial matters. [179]

Although these reasons have been and still are under discussion, this thesis will only focus on the criminal concerns the PBOC initially alleged. It is important to emphasize that China's pivotal role in the arena of cryptocurrencies entailed that the country was also plunged as a victim of cryptocurrency-related crime. As section 4.1. established, the Chinese government partially based the crypto ban on a series of crimes that were

---

[175] Team C, "East Asia: Pro Traders and Stablecoins Drive World's Biggest Cryptocurrency Market" (*Chainalysis* May 20, 2022) <https://blog.chainalysis.com/reports/east-asia-cryptocurrency-market-2020/> accessed December 2, 2022

[176] Ibid Lima (192)
[177] Ibid Lima (192)
[178] Asian Racing Federation, 2021 ' How China's Crackdown on Illegal Betting Impacts Global Betting Markets' https://assets-global.website-files.com/5fbe2bde2b2ef4841cd6639c/612df2b7fc6bc25c218b6a54_How%20China%27s%20Crackdown%20on%20Illegal%20Betting%20Impacts%20Global%20Betting%20Markets.pdf
[179] Xie Rain, 'Why China had t Why China had to "Ban" Cryptocurrency but the US did not: A ency but the US did not: A Comparative Analysis of Regulations on Cr e Analysis of Regulations on Crypto-Markets Between ets Between the US and China ' [2019] 18(2) Washington University Global Studies Law Review

concerning the government because of their impact on Chinese society and citizens. Among these, the ones that were decisive for the banning are:

1. Fraud in ICOs: a report published by Reuters in 2021 concluded that $2.2 billion worth of cryptocurrencies were sent, and two billion received, from Chinese addresses to others associated with illicit activities such as frauds, frauds, and darknet operations. [180]

2. Money laundering: Billions of dollars have been laundered through cryptocurrencies. For instance, money from fentanyl trafficking (of which China is the number one trafficker), or hacking (as in the case of Tian Yinyin and Li Jiadong, two Chinese nationals who laundered more than 100 million worth of cryptocurrencies to hide the money they received by helping North Korean hackers to launder almost two billion worth of cryptocurrencies they had stolen allegedly from the North Korean government.) [181]

3. Risk to financial stability, and consumers.

4. Tax evasion.

The following section aims to explain the regulatory approach that China has adopted, particularly concerning these offenses.

4.2 Money Laundering and Terrorism Financing Regulation.

This chapter discusses how money laundering and terrorist financing were the two cryptocurrency-related crimes that China was most concerned about. This, coupled with the fact that both crimes are considered extremely serious in the country, may explain why China has enacted numerous policies.

---

[180] Person R and Chavez-Dreyfuss G, "Chinese Crypto Addresses Sent $2.2 Bln to Scams, Darknets in 2019-2021 -Report" (*Reuters* August 3, 2021) <https://www.reuters.com/technology/chinese-crypto-addresses-sent-22-bln-scams-darknets-2019-2021-report-2021-08-03/> accessed December 2, 2022

[181] "China Primer: Illicit Fentanyl and China's Role - Congress" < https://crsreports.congress.gov/product/pdf/IF/IF10890> accessed December 2, 2022
"Two Chinese Nationals Charged with Laundering over $100 Million in Cryptocurrency from Exchange Hack" (The United States Department of Justice July 22, 2022) < https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack> accessed December 2, 2022

The regulation of money laundering and terrorist financing in China is characterized by laws of general application that already existed when cryptocurrencies emerged, and that after their appearance in the market were included in the material scope.

4.2.1 The Anti-Money Laundering Law of the People´s Republic of China (Decree No. 1 of 2006 of the People's Bank of China). [182]

As in the European Union, China enacted this Decree to curb its history of money laundering and related crimes (drug trafficking, embezzlement, bribery, illegal arms sales, organized crime, etc.).[183] Initially, money laundering was only included in the Criminal Code in 1997. However, in 2003, as a result of events such as 9/11, China, like other countries, decided to enact stricter and more specific legislation. In this way, not only was it anticipated to penalize these conducts, it also began to create legal instruments that would establish measures to combat them. Thus, in the year 2006, the Chinese Anti-Money Laundering Law was enacted, which is the main legislation to address money laundering in China. Within its scope of application, it does not exclusively regulate money laundering exclusively, but Article 2 clarifies that the measures displayed throughout the text are also applicable to related crimes such as drug-trafficking, terrorist crimes, or crimes committed by organizations. Furthermore, this law sets out the principles and general requirements for the prevention and control of money laundering for any company or organization operating in China, especially in financial matters. Considering cryptocurrencies are highly related to financesany related activity must comply with this law.

The AML of China would be comparable to the European Union´s 5th Anti-money Laundering Directive as it is the main regulation on money laundering. Nonetheless, it is not the only regulation on this matter. Of those enacted by the PBOC, and whose scope of application includes cryptocurrencies, the '*Foreign Exchange Administration Regulation'* and '*The Banking Law'* should be highlighted. The first one establishes the rules for the purchase and sale of foreign exchange and other financial assets in China, which includes cryptocurrencies. 'The Banking Law' regulates the activities of banks in China, establishing a series of requirements for the prevention of money laundering and

[182] 'Anti-Money Laundering Law of the People's Republic of China (Adopted at the 24th Meeting of the Standing Committee of the Tenth National People's Congress on October 31, 2006)' (*NPC Government*) accessed 14 May 2023
[183] Ibid.

financing of terrorism. [184] Although the law does not specifically address cryptocurrencies, it is important to note that financial institutions are subject to the regulations of the PBOC. As explored earlier, the PBOC issued measures to restrict cryptocurrency trading on local platforms and limit cross-border cryptocurrency transactions.

As has been reiterated throughout this thesis, cryptocurrencies have criminal potential, because they are susceptible to being used for illicit purposes. In the case of money laundering, it was established that the lack of intermediaries due to decentralization and anonymity were incentives to commit crimes such as money laundering. To combat these characteristics, a series of common measures can be found in the AML-regulationhave been set forth: [185]

1. All institutions, financial or not, are required to establish an AML reporting entity. These entities are responsible for carrying out the task of prevention and detection of money laundering activities.

2. Customer identification: Financial institutions, including cryptocurrency exchange houses, must conduct due diligence on their customers and verify their identity before conducting any transactions. For example, cryptocurrency exchanges must verify the identity of users before allowing them to perform transactions. Furthermore, these institutions are compelled to regularly assess due diligence and to re-identify their customers in cases of suspicion.

3. Transaction monitoring: Financial institutions should continuously monitor transactions conducted by their customers to detect possible suspicious money laundering activities. For example, cryptocurrency exchanges must continuously monitor cryptocurrency transactions made by their users.

4. Suspicious Transaction Reporting: Financial institutions should report to the competent authorities in case of detecting suspicious money laundering transactions. Along with the activities that are considered suspicious, it is possible to mention that the customer refuses to validly identify himself or that the

[184] Zhou S and Leimin Y, 'Anti Money Laundering Laws and Regulations Report 2022-2023 China' (International Comparative Legal Guides International Business Reports, 2022) accessed 16 May 2023
[185] Ibid.

transactions of cryptocurrencies carried out exceed the thresholds established by the authorities.

5. Risk Assessment: AML Reporting Entities should conduct a risk assessment of the activities of their customers to identify money laundering activities and take preventive measures.
6. Staff Training: Financial institutions should train their staff concerning applicable laws and regulations to prevent and control money laundering.
7. Record Keeping: AML Reporting entities should maintain accurate and complete records of all transactions conducted by their customers, including those related to cryptocurrencies.
8. Cooperation with authorities: Financial institutions should cooperate with competent authorities in the investigation and prevention of activities related to money laundering and terrorist financing. [186]
9. Penalties: Violations of any of these measures can lead to administrative and criminal sanctions.

As can be noticed, the measures are like those adopted by the European Union. Through the measures to identify the users of cryptocurrencies, the criminal advantage that anonymity offers are eliminated. Likewise, by introducing an anti-money laundering reporting entity, a third-party intermediary is introduced, which despite not having any participation in the transactions, exercises supervision that reduces the risks inherent to the decentralization of cryptocurrencies. All these measures may lead to greater control over cryptocurrencies, and over the elements that bring out their criminogenic potential. This counteracts the grounds why many criminals adopt them as a criminal means.

4.2.2 The Counterterrorism Law of the People´s Republic of China (Order No.36 of the president of the PCR). [187]

[186] Zhou S and Leimin Y (177)

[187] Counterterrorism Law of the People's Republic of China (Order No. 36 of the President of the PRC).英文译本 - 北大法宝V6" (*英文译本 - 北大法宝V6*) <http://en.pkulaw.cn/>. accessed 16 May 2023

In its fight against terrorism, China maintains a preemptive and permanent crisis approach, maintaining a constant state of alert. Thus, it is easier tackle a threat in a more effective and quick manner.

The Counterterrorism Law was enacted by President Xi Jinping in 2015 under the ideology of fighting the so-called three forces of evil: ethnic separatism, religious extremism, and violent terrorism. This legislation enumerates a series of measures to prevent, repress and punish terrorist acts.[188] Internationally, it has been considered extremely strict legislation, since along with its measures, it allows the Chinese authorities to conduct surveillance and monitoring, including access to communications data of citizens, and has prohibited the use of encryption devices that cannot be unlocked by the authorities.[189] Along with the money laundering law, it is the key legislation to combat these offenses. The law established the Financial Intelligence Unit that are specialized in detecting and preventing the financing of terrorism. [190] It also advocates international cooperation to combat terrorist financing. China has joined the UN international convention for the Suppression of the Financing of Terrorism, as well as the Eurasia Group on money laundering and terrorist financing, the Asia Pacific Group on money laundering, and the Financial Action Task Force. [191]

Furthermore, the law includes provisions related to the prevention and control of terrorist financing. For instance:

- The monitoring of financial and funds transfers. These institutions, as in the money laundering law, are subject to strict regulations regarding the supervision and monitoring of suspicious financial transactions.
- In cases of suspicious activity or transactions related to terrorism, financial institutions have the duty of reporting.

[188] Márquez M, 'La Estrategia Contraterrorista de La República Popular China En Xinjiang' (Instituto Español de Estudios Estratégicos , 14 November 2022) accessed 16 May 2023
[189] Amnistía internacional, 'China: La ley de seguridad nacional no debe convertirse en instrumento de miedo' (*Aministía Internacional*, 20 June 2022) <https://www.amnesty.org/es/latest/news/2020/06/china-national-security-law-weapon-of-fear/> accessed 16 May 2023
Ben Blanchard, 'China aprueba una controvertida ley antiterrorista' (*Reuters* , 28 December 2015) <https://www.reuters.com/article/china-seguridad-ley-idESKBN0UB0EE20151228> accessed 16 May 2023
[190] China´s Response to Terrorism. (Channel New Asia Analysis / Solutions, June 2016). https://www.uscc.gov/sites/default/files/Research/Chinas%20Response%20to%20Terrorism_CNA061616.pdf
[191] Ibid.

- The Chinese government has the authority to freeze financial assets and apply sanctions to individuals and organizations involved in terrorist activities, this includes prohibiting financial transactions. [192]

It is possible to observe that the measures in the counter-terrorist financing law are in line with those provided in the anti-money laundering law. Nonetheless, in case of the former, the emphasis is placed more on the monitoring of transactions and international cooperation. This is probably because the Chinese authorities have given importance to the transnational nature of cryptocurrencies and the crimes related to them. This may counteract the fact that there are legislative differences between jurisdictions. Although, as we have seen, cryptocurrencies do not have the same legal status in all countries, countries have common objectives, such as for example avoiding the financing of terrorism. With international cooperation policies, it is easier to prevent and prosecute these crimes. [193]

4.2.3 Measures for the Supervision and Administration of Anti-Money Laundering and Counter-Terrorist Financing of Financial Institutions. [194]

Following the enactment of AML and CT laws, the PBOC has presented other legal instruments that aim to create specific standards and guidelines to implement a series of money laundering and terrorist financing prevention procedures and protocols. The most relevant complementary laws in China are the so-called ‘Measures,’ which were enacted in mid-2021 by the PBOC. [195] These measures are targeted at financial institutions and their effective compliance with anti-money laundering and anti-terrorism laws explored earlier. What is interesting about these measures is that they govern investment, securities,

[192] PBC, gov, 'Anti-Money Laundering and Combating Terrorist Financing´ (*Pbcgov English Sources: Annual Report* , 2007) <http://www.pbc.gov.cn/english/resource/cms/2015/10/2015102917103229547.pdf> accessed 16 May 2023

[193] Tetyana Semigina and Galyna Muliar , Association Agreement: Driving International Changes (Accent Graphics Communications 2019) 235-243

[194] Simon Fung hui , 'China: China expands anti-money laundering obligations with Measures for the Supervision and Administration of Anti-Money Laundering and Counter-Terrorist Financing of Financial Institutions' (*Baker McKenzie Global Compliance News* , 20 August 2021) <https://www.globalcompliancenews.com/2021/08/20/china-expands-anti-money-laundering-obligations-with-measures-for-the-supervision-and-administration-of-anti-money-laundering-and-counter-terrorist-financing-of-financial-institutions090821/> accessed 13 May 2023

[195] Ibid.

and asset management companies, foreign exchange institutions, and other non-banking payment institutions. [196]

In this legislation, the PBOC decides to adopt the international regulatory stance and implements a risk-based approach to combat and prevent this kind of crime. The European Union has also adopted this approach. The risk-based approach aims to assess the risks associated with these crimes and to implement preventive measures to mitigate them. [197]

The measures include the following obligations for financial institutions: [198]

- establish an internal control system aimed at preventing money laundering and terrorist financing.
- set up risk self-assessment systems. Furthermore, these systems should be evaluated on a regular or random basis. There is an obligation to report the results of these assessments to the PBOC.
- together with the self-risk-assessment systems, establish an audit mechanism by an independent external auditor to evaluate their systems;
- implement KYC measures, identifying and verifying the identity of customers. It is recommended to do this through reliable means of information (Passport, ID).
- in transactions (e.g., bitcoin), the purpose and nature of such financial activity should be understood.
- in case of an elevated risk that a transaction could be used for money laundering or terrorist financing, information on the origin and use of customer funds should be obtained. Adjacent to this, due diligence standards should be implemented;
- customers and their transactions should be monitored regularly;

[196] Simon Fung Hui , 'Legal Update: China Expands Anti-Money Laundering Obligations with Measures for the Supervision and Administration of AML/CTF of Financial Institutions' (*Baker McKenzie Global Compliance News* , 15 September 2021) <https://financialinstitutions.bakermckenzie.com/2021/09/15/china-expands-anti-money-laundering-obligations-with-measures-for-the-supervision-and-administration-of-aml-ctf-of-financial-institutions/> accessed 13 May 2023.
[197] The regtank team, 'What is Risk-Based Approach and Why Is It Important ' (*What is Risk-Based Approach and Why Is It Important* , 25 March 2021) <https://regtank.com/what-is-risk-based-approach-and-why-is-it-important/> accessed 13 May 2023
[198] Ibid.

— verify that the services and transactions performed by the client are by the background information they have. In this vein, the customer should not only be identified, but also the beneficiary of the transactions carried out, and in the cases of a legal person or an unincorporated organization, its authenticity should be verified.

— have an IT system trained to tackle money laundering and financing of terrorism matters. This system should be updatable regularly.

— facilitate on-site inspections of the PBOC. This includes the authority to verify and copy records and materials, relating to the management of the institution regarding their money laundering and financing risk management system. [199]

As can be noted, thesemeasures seek to neutralize the risks that may arise from the misuse of cryptocurrencies. Firstly, because these measures are not reactive, but preventive and control measures. They require the intervention of a third party in Bitcoin transactions, which counteracts the attractiveness of decentralization. All transactions are monitored, associated with a person, and their nature is required to be understood, thus, reducing the possibility of cryptocurrencies being used as a means of ML or TF. Likewise, as observed in other legislation, KYC measures nullifies the anonymity of cryptocurrencies, Finally, enforcing a a system of sanctions, encourages these institutions toto comply with the legislation, while acting diligently in their operations.

4.3 Regulation regarding fraud and embezzlement offenses.

Concerning fraud and embezzlment, much of the regulation that China has enacted has already been discussed: the banning of the ICOs in 2017, the prohibition of mining, and the outlawing of all cryptocurrency business activities in 2021. These are all regulatory measures that were taken, among other reasons, to combat the challenges raised by the criminogenic potential of cryptocurrencies. In this case, the concern of the Chinese

[199] Ibid.
Conventus law , 'China – Measures For The Supervision And Administration Of Anti-Money Laundering And Anti-Terrorist Financing Of Financial Institutions' (*Conventus Law* , 20 July 2021) <https://conventuslaw.com/report/china-measures-for-the-supervision-and-2/#:~:text=In%20order%20to%20cause%20financial%20institutions%20to%20effectively,Anti-Terrorism%20Law%20of%20the%20People%E2%80%99s%20Republic%20of%20China.> accessed 13 May 2023

authorities focused on protecting their citizens from potential fraud, as well as maintaining the integrity of the market and protecting consumers.

Of the regulations already explored, it is essential to delve a little deeper into the prohibition of ICOs, since the *Announcement on the Prevention of Financial Risks of Token Issuance* declared that the ban was in response to the fraud crimes that China was suffering from. [200] The purpose of this Announcement, as already discussed, according to the Chinese authorities was to mitigate *`the illegal fund-raising, financial fraud, pyramid scheme, and other criminal activities´* that came from the use of the ICOs. [201] This ban is relevant to explore, not only because it explains China´s regulatory stance on cryptocurrencies, but also because of the legal implications that flowed from it. The ban on ICOs brought with it the closure of cryptocurrency exchange platforms. For instance: Bitcoin, OkCoin, and Huobi closed that September of 2017 due to the potential risk of fraud. The ban has led to the closure of cryptocurrency platforms such as BISS, which was involved in fraudulent activities. [202] In the wake of the ICO ban, China began to bring greater regulatory scrutiny to the country, leading to stricter measures being implemented to prevent potential fraud and protect investors and consumers. For instance, the Cryptocurrency Advertising Ban or the 2017 cryptocurrency exchange prohibition. The first one because it made platforms and social networks to be subject to strict regulations aiming to prevent misleading advertising and the promotion of fraudulent schemes. The second one is because these exchange platforms were forced to cease their operations. The following sections will discuss some laws that complete the regulations already explored.

As in the rest of the world´s jurisdiction, the most common cryptocurrency-related frauds have been investment schemes and rug pull scams. The first is aimed at getting citizens to invest in cryptocurrencies under the promise that they are going to obtain financial gains, however, these cryptocurrencies are fraudulent (as in the One Coin Case). The second fraud consists of obtaining funding to carry out a (non-existing) project. [203]

---

[200] Stan Schroeder , 'China bans ICOs for being full of fraud and pyramid schemes' (*Mashable* , 4 September 2017) <https://mashable.com/article/china-bans-icos-bitcoin> accessed 13 May 2023

[201] Ibid

[202] Bradley Noah , 'BISS exchange in China shut down as governments launch anti-crypto assault' (*CoinGeek* , 25 November 2019) <https://coingeek.com/biss-exchange-in-china-shut-down-as-governments-launch-anti-crypto-assault/> accessed 16 May 2023

[203] Hetler A, '10 Common Cryptocurrency Scams in 2023' (*WhatIs.com*, 19 April 2023) accessed 15 May 2023

Although it has been already discussed, the regulatory impact that investment frauds have had on the Chinese regulatory approach regarding cryptocurrencies, it is necessary to highlight the relevance of the named ´rug-pull scams´, since, according to the Chainalysis Report, in 2021 they were 37% of the illicit revenue in China. [204] It is estimated that China lost around three billion dollars in such scams, which has had a regulatory significance. [205]

4.3.1 Legal Interpretation (2022) No. 5 The Decision of the Supreme People's Court on Amending the Interpretation of the Supreme People's Court on Several Issues Concerning the Specific Application of Law in the Trial of Criminal Cases of Illegal Fund-raising. [206]

On February, 2022, the Supreme Court of China ruled that certain virtual currency transactions are going to be considered a crime of illegal fund-raising or illegally absorbing funds, which is a prosecutable punishable offense under the Criminal Law of China. Indeed, its perpetration entails a fine ranging from 80.000 dollars to 10 years of imprisonment (Art. 176).[207]

One of the rationales provided by the court in the ruling is the number of fund-raising frauds that are occurring involving cryptocurrencies. In September 2022, the country registered 25.000 cases of fraudulent fund-raising in the last five years related to virtual currencies.[208] Therefore, the Supreme Court has been forced to include virtual currencies under the scope of application as a criminal means for the commission of this offense.

Therefore, under the new ruling, any fund-raising related to cryptocurrencies that do not establish and identify its purpose, which promotes returns of capital or interest, or that aims to sell or exchange commodities, and other series of activities will be considered a

---

[204] ‘ 中国人民银行 中央网信办 工业和信息化部 工商总局 银监会 证监会 保监会关于防范代币发行融资风险的公告’ (*pbc.gov.cn*) accessed 16 May 2023

[205] Ibid.

[206] Supreme People’s Court of the People´s Republic of China, ‘Decision of the Supreme People’s Court on Amending the Interpretation of the Supreme People’s Court on Several Issues Concerning the Specific Application of Law in the Trial of Criminal Cases of Illegal Fund-Raising.’ (*权威发布 - 中华人民共和国最高人民法院*) accessed 15 May 2023

[207] Ibid.

[208] Pandadaily , 'Chinese Authorities Crack Down on $56B Crypto-Related Money Laundering' (*Panda Daily* , 27 September 2022) <https://pandaily.com/chinese-authorities-crack-down-on-5-6b-crypto-related-money-laundering/> accessed 14 May 2023

criminal offense. Including cryptocurrencies under the scope of this regulation can prevent frauds such as rug pull scams, by which projects, companies, and even charities are seeking to be financed with cryptocurrencies.

Although criminal law is not the panacea for combating crime, nor does it imply the total suppression of the commission of these offenses, or in this case, the elimination of the use of criminal means such as cryptocurrencies. Nonetheless, it indeed has a preventive and deterrent aspect. [209] In the same vein, it can alert citizens, inviting them to be more cautious when investing in cryptocurrencies. [210] These two elements can lead to the reduction of the criminogenic potential of cryptocurrencies.

4.4 Other regulatory initiatives: Techno-regulation and awareness campaigns.

Along with the promulgation of these regulations, the Chinese authorities have decided to adopt a proactive role in their enforcement to fight against cryptocurrency-related crimes. And they have carried it out in two ways:

1. Through techno-regulation: China uses what is known as the ´Great Firewall´, which is a system composed of proxy servers and firewalls that block Internet content. It is considered a policy that combines technology and law. [211] This, for instance, has been used to enforce the prohibition of cryptocurrency advertising. Furthermore, it has been used to combat other crimes involving cryptocurrency such as illegal gambling or money laundering. At first, these illegal transactions were being carried out through VPN networks, however, the government utilized the Great Firewall to detect the VPN and block the server to which it is connected. It should be noted that techno-regulation is a method frequently employed by China and one that has succeeded in mitigating criminal actions. [212]

[209] Fernando Miró llinares and Rebeca Bautista ortuño, 'Por qué cumplimos las normas penales? Sobre la disuasión en materia de seguridad vial' [2013] 4(2013) InDret: Revista para en Análisis del Derecho <https://indret.com/wp-content/themes/indret/pdf/1001.pdf> accessed 15 May 2023
[210] Michael Pawlik , Ciudadanía y Derecho Penal: Fundamentos de la teoría de la pena y del delito en un Estado de libertades (Atelier 2016)
[211] “Great Firewall” (WikipediaNovember 26, 2022) <https://en.wikipedia.org/wiki/Great_Firewall> accessed December 2, 2022. Putro, “VPN Compliance in China” (*Law.asia* March 8, 2021) <https://law.asia/vpn-compliance-china/> accessed December 2, 2022
[212] Ibid

2. Awareness-raising campaigns. In November 2019, the Chinese government launched a media campaign to combat fraud occurring in the name of cryptocurrencies. The government claimed that from the 32.000 projects that were claiming to use blockchain and cryptocurrencies, less than 10% of those firms were using or working with the technology. [213] Although it is not a regulatory measure *per se,* it is a measure that seeks to combat crimes associated with the illicit use of cryptocurrency. Certainly, it warns citizens who use cryptocurrencies, which may reduce the possibility of them falling into fraud or Ponzi Schemes.

4.5 Conclusion.

China's regulatory framework is stricter than that of the EU, having practically banned cryptocurrencies in the country. However, the regulatory measures can be considered in line with those discussed in Chapter 3. China is aware of the criminogenic potential of cryptocurrencies, and that is why it includes them under regulations such as anti-money laundering or counterterrorism or even creates campaigns exclusively dedicated to warning about these risks. The legislation discussed focuses on the elements of decentralization and anonymity and tries to attack them through the law, requiring customer identification, transaction monitoring, and risk assessment measures. It also focuses on the importance of international cooperation to combat these crimes of an international nature. Although all economic operations with cryptocurrencies are prohibited in the country, it is interesting to note that China has continued to regulate them.

Chapter 5. Conclusions.

At the beginning of the thesis, the question was posed as follows:

Faced with the criminogenic potential of cryptocurrencies, what are the regulatory approaches employed by the European Union and China to prevent and mitigate the commission of such crimes?

[213] Genny Diaz , 'China emprende campaña para combatir estafas asociadas a blockchain y criptomonedas' (Criptonoticias , 19 November 2019) <https://www.criptonoticias.com/comunidad/china-emprende-campana-blockchain-criptomonedas/> accessed 13 May 2023

To answer this question, the different chapters have analyzed the regulations of the jurisdictions, as well as the role of cryptocurrencies and their potential criminogenic use. Some points can be concluded from this analysis:

1. Both countries differ culturally, economically and politically. Therefore, it may be reasonable to infer that these differences cause different reactions to the same phenomenon, such as cryptocurrencies and their illicit use. Let us remember that cryptocurrencies are decentralized and anonymous, and that while their use can be advantageous in society, as this thesis has shown, they can be used to commit numerous crimes, such as the financing of terrorism or money laundering.

2. In the case of the European Union, regulation, the promulgation of norms, predominates in order to tackle the criminogenic potential. The EU considered cryptocurrencies legal, as a technology that can be adopted and commercialized, but which need a series of regulatory limits, to mitigate the potential hazards related to the misuse of cryptocurrencies.

3. China, on the other hand, does not only employ regulation: prohibiting practically all commercial activities with cryptocurrencies. Only their ownership is legal. Rather, it employs techno regulation to ensure enforcement such as the use of The Great Firewall.

4. Although cryptocurrencies in each jurisdiction have a different legal status, their regulation to alleviate the criminality of their illicit use is very similar, not to say that many of these regulations are similar:

    a. For instance, to alleviate anonymity, user identification measures (KYC) are required. It is required to check the background of crypto users. Thus, illegal transactions are prevented, since it is necessary for the institutions providing crypto related services to not only identify their costumer, but to understand the nature and purpose of their transactions, and check if their activity is in accordance with the background presented. It is even required to know the identity of the recipient (in the case of China).

    b. Decentralization, while it remains in the way that cryptocurrencies and the blockchain operate, is removed by creating third parties that must monitor transactions, report them and watch for suspicious activities. It is no longer

just a communication between sender and receiver. If not, there is a third-party observer of those transactions.

5. Likewise, both jurisdictions propose a system of licenses or registrations to control the services and institutions that operate with cryptocurrencies. Another common regulatory point is having established specialized agencies (FIU) to carry out the implementation of these measures.

6. Both countries emphasize the importance of international cooperation as a measure to combat these crimes. The fact that cryptocurrencies have different legal statuses could imply that criminals could offend in laxer jurisdictions. However, if countries with different regulatory approaches have the same objective and cooperate, it is easier to prosecute these crimes. Finally, the EU and China have implemented has been the imposition of sanctions on companies or financial institutions that provide cryptocurrency services.

Concluding, even though the regulatory background is different the regulatory approach taken to tackle some crimes can be very similar. The main difference is that China's approach is stricter regarding the use of cryptocurrencies. However, both regulatory approaches are based on preventing these crimes from occurring, and reacting when the illegal conducts take place.

Bibliography.

- Commission ‘Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets and amending Directive (EU) 2019/1937 COM (2020) 593 final.
- Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ 2 156/43
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ 2 141/74
- Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 5
- *Högsta förvaltningsdomstolen* [2016] European Parliament, 52 C-264/14 ECLI:EU:C:2015:718
- K Bilz and Nadler J, Chapter 10: Law, Moral Attitudes and Behavioral Change. in E Zamir and D Teichman (eds), The Oxford Handbook of Behavioral Economics and the Law (OUP USA 2014) 241
- A Prytula and others, 'Cryptocurrency in transnational offenses: criminal and civil legal aspects Anatolii Prytula' [2021] 10(2322-6307) Amazonia Investiga.
- Andrea Gaggioli, 'Blockchain Technology: Living in a Decentralized Everything' [2018] 21(1) CyberSightings.
- Agbo Elias Igwebuike, 'Cryptocurrency and the African Economy ' [2020] 2(5282 - 0053) Economic and Social Science Academic Journal.
- Beatriz Garcia moreno and Adán Nieto martín, 'Criptomonedas y derecho penal: más allá del blanqueo de capitales' [2021] 23(17) Revista Electrónica de Ciencia Penal y Criminología.
- Brian Donohue, 'The Wonders of Hashing' (*Kaspersky Daily*, 10 April 2014) <https://www.kaspersky.com/blog/the-wonders-of-hashing/4441/> accessed 8 June

- Casey Murphy, 'Bitcoin Scams: How to Spot Them, Report Them, and Avoid Them' (*Investopedia*, N/D) <https://www.investopedia.com/articles/forex/042315/beware-these-five-bitcoin-scams.asp> accessed 3 July 2022
- Covadonga Mallada, 'La financiación del terrorismo desde la perspectiva de las nuevas tecnologías A propósito de la quinta Directiva de la UE de prevención del blanqueo de capitales y la financiación del terrorismo' [2018] 71(1) Universidad de Valladolid
- David Lee and others, 'Cryptocurrency: A new investment opportunity?' [2018] 20(3) Institutional Knowledge at Singapore Management University <10.3905/jai.2018.20.3.016> accessed 7 June 2022
- Digital Shadow 'A Tale of Epic Extortions - How Cybercriminals Monetize Our Online Exposure' (*Digital Shadows* 2019) <https://resources.digitalshadows.com/whitepapers-and-reports/a-tale-of-epic-extortions-how-cybercriminals-monetize-our-online-exposure> accessed 11 July 2022
- MA García-ramos lucero and R Rejas muslera , 'Análisis del desarrollo normativo de las criptomonedas en las principales jurisdicciones: Europa, Estados Unidos y Japón' [2022] 35(ISSN 1699-8154) Revista de Internet, Derecho y Política
- Marten Risisus and Kai Spohrer, 'A blockchain research framework: What We (don't) Know, Where We Go from Here, and How We Will Get There' [2017] 59(1) Business & Information Systems Engineering.
- Meng Qin, Chi-Wei Su and Ran Tao, 'Bitcoin: A New Basket For Eggs?' (2021) 94 Economic Modelling.
- Michael Comiskey and Pawan Madhogarhia, 'Unraveling the Financial Crisis of 2008' [2009] 42(2) PS: Political Science and Politics.
- Jorge Izaguirre , 'Análisis de los Ciberataques Realizados en América Latina' [2018] 3(9) Universidad Internacional del Ecuador 180-189
- W. Arner Douglas, 'The Global Credit Crisis of 2008: Causes and Consequences [2009] 43(1) The International Lawyer - American Bar Association 91-136.
- Chainalysis, '2019 Crypto Crime Report: Decoding Hacks, Darknet Markets and Scams', (Chainalysis, 2019)
- Chainalysis, '2022 Crypto Crime Report: Original Data and Research Into Cryptocurrency-Based Crime, (Chainalysis, 2022)

- Europol, ‘Europol Spotlight: Cryptocurrencies tracing the evolution of criminal finances’ (Europol, 2022)
- Financial action task force, 'Virtual Currencies Key Definitions and Potential AML/CFT Risks' (*FATF-GAFI*, June 2014)
- Financial action task force, 'GUIDANCE FOR A RISK-BASED APPROACH VIRTUAL CURRENCIES' (*FATF-GAFI*, June 2015)
- Financial action task force, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Provider' (*FATF-GAFI*, June 2019)
- Financial Crimes Enforcement Network and United States Department of the Treasury, ‘Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime’, (FinCEN, 2016).
- González Marta, ‘Fiscalidad aplicable a los bitcoines a la luz del ordenamiento tributario español’ (AEDAF Revista Técnica Tributaria, 2017)
- Thomson Reuters, ‘Cryptocurrency regulations by the country report’, (Thomson Reuters, 2022)
- United Nations Office On Drugs and Crime, ‘The Counter Terrorism Legal Training Curriculum’, (UNODC, 2017)
- Ayudaley, 'Derecho a la privacidad en España Guía 2021' (*Ayudaley Protección de Datos*, N/D) <https://ayudaleyprotecciondatos.es/2018/11/13/derecho-privacidad-espana/#Derechos_relativos_al_ambito_privado> accessed 2 July 2022
- Anthony Minnaar, 'ORGANISED CRIME AND THE ‘NEW MORE SOPHISTICATED’ CRIMINALS WITHIN THE CYBERCRIME ENVIRONMENT: HOW ‘ORGANISED’ ARE THEY IN THE TRADITIONAL SENSE?' (*Academia Edu* , 2019) <https://www.academia.edu/40211446/ORGANISED_CRIME_AND_THE_NEW_MORE_SOPHISTICATED_CRIMINALS_WITHIN_THE_CYBERCRIME_ENVIRONMENT_HOW_ORGANISED_ARE_THEY_IN_THE_TRADITIONAL_SENSE> accessed 15 July 2022
- Bit2me, 'What is double spending' (*Bit2me Academy*, N/D) <https://medium.com/@ipspecialist/how-blockchain-technology-works-e6109c033034> accessed 12 June 2022
- C Mridusmita, 'The Financial Crisis 2008 Explained in Simple Terms' (*Economyria*, September 29, 2016) <http://economyria.com/the-financial-crisis-2008-explained/> accessed 1 June 2022.

- Chabaneix, 'Delitos de estafa y blanqueo de capitales con criptomonedas' (*Abogacía Española Consejo General* , N/D) <https://www.abogacia.es/publicaciones/blogs/blog-subcomision-prevencion-blanqueo-capitales/delitos-de-estafa-y-blanqueo-de-capitales-con-criptomonedas/> accessed 3 July 2022
- Daniels Lyons , 'European Court of Justice rules that Bitcoin should be treated as a currency for VAT purposes' (Deloitte, 22 October 2015) <https://www2.deloitte.com/uk/en/pages/press-releases/articles/european-court-rules-bitcoin-be-treated-as-currency-for-vat.html> accessed 7 November 2022
- Despacho ferrer-bonsoms &sanjurjo , 'Regulación de blockchain y criptomonedas en la Unión Europea' (*Despacho Ferrer-Bonsoms &Sanjurjo* , N/D) <https://ferrer-bonsoms.com/regulacion-de-blockchain-y-criptomonedas-en-la-union-europea/> accessed 29 August 2022
- Edward Kost , 'Ransomware Attacks Vs Data Breaches: What's the Difference?' (*Upguard*, N/D) <https://www.upguard.com/blog/ransomware-attacks-vs-data-breaches> accessed 2 July 2022
- European central bank, 'What is bitcoin? ' (*ECB Europa*, 13 February 2018) <https://www.ecb.europa.eu/ecb/educational/explainers/tell-me/html/what-is-bitcoin.en.html> accessed 7 June 2022
- European Council , 'Digital finance: agreement reached on European crypto-assets regulation (MiCA)' (*Consilium Europa EU* , 30 June 2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/> accessed 29 August 2022
- Ibm , ' What is blockchain technology? ' (*IBM*, N/D) <https://www.ibm.com/topics/what-is-blockchain> accessed 8 June
- Ip specialist, 'How Blockchain Technology Works' (*Mediumcom*, 15 October 2019) <https://medium.com/@ipspecialist/how-blockchain-technology-works-e6109c033034> accessed 12 June 2022
- J. Khangura and J. Arora, "A Study on Security Threats to Blockchain & Cryptocurrencies," 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), 2021, pp. 1560-1564, doi: 10.1109/ICAC3N53548.2021.9725412.

- Jacek Czarnecki , 'Cryptocurrency a financial instrument? A new proposal in the EU' (*Newtechlaw*, 1 October 2018) <https://newtech.law/en/cryptocurrency-a-financial-instrument-a-new-proposal-in-the-eu/> accessed 29 August 2022
- Javier Martín del barrio , 'La autoridad bancaria europea alerta de los peligros del bitcoin' (*El País* , 13 December 2013) <https://elpais.com/tecnologia/2013/12/13/actualidad/1386926648_816453.html> accessed 29 August 2022
- Jp morgan chase & co, 'Could Blockchain Have as Great an Impact as the Internet?' (*JP Morgan Chase & Co*, N/D) <https://www.jpmorganchase.com/news-stories/could-blockchain-have-great-impact-as-internet> accessed 15 June 2022
- Kimberly Amadeo, 'Causes of the 2008 Global Financial Crisis ' (*The Balance*, January 17, 2022) <https://www.thebalance.com/what-caused-2008-global-financial-crisis-3306176> accessed 1 June 2022.
- Kyle Lee, 'What Is Decentralization?' (*Studycom*, 24 March 2022) <https://study.com/learn/lesson/decentralization-concept-examples.html> accessed 7 June 2022
- McAfee, 'Informe sobre amenazas contra blockchain' (Mc Afee, June 2018) <https://www.mcafee.com/enterprise/es-es/assets/reports/rp-blockchain-security-risks.pdf> accessed 1 June 2022
- M Harrigan, 'An Analysis of Anonymity in the Bitcoin System' [2012] 3(1) 11Clique Research Cluster, Complex & Adaptive Systems Laboratory, University College Dublin, Ireland <10.1109/PASSAT/SocialCom.2011.79> accessed 7 June 2022
- Marie Huillet, 'Informe: Hackeo de Coincheck perpetrado por un virus vinculado a hackers rusos' (*Cointelegraph*, 17 June 2019) <https://es.cointelegraph.com/news/report-record-breaking-coincheck-hack-perpetrated-by-virus-tied-to-russian-hackers> accessed 1 June 2022.
- M Möser, 'Anonymity of Bitcoin Transactions An Analysis of Mixing Services' (University of Münster, 2013) <https://www.wi.uni-muenster.de/sites/wi/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf> accessed 7 June 2022
- Luis Esparragoza, 'Hace 10 años nació Silk Road, primer mercado de la dark web que aceptó bitcoin' (*Criptonoticias* , 27 January 2021) <https://www.criptonoticias.com/comunidad/10-anos-nacio-silk-road-primer-mercado-darkweb-acepto-bitcoin/> accessed 2 September 2022

- Samuel Haig , 'China crypto crime: Still ‘top ranked’ for illicit activity, but crime is falling' (*Cointelegraph* , 04 August 2021) < https://cointelegraph.com/news/china-crypto-crime-still-top-ranked-for-illicit-activity-but-crime-is-falling > accessed 5 September 2022
- Satoshi Nakamoto, 'Bitcoin: A Peer-To-Peer Electronic Cash System' (*Bitcoin.org*, 2008) <https://bitcoin.org/bitcoin.pdf> accessed 1 June 2022.
- Spamfighter, 'Latest Extortion Email threatens to send Hitman unless ransom amount in the form of Bitcoin is paid' (*Spam fighter* , 2019) <https://www.spamfighter.com/News-21969-Latest-Extortion-Email-threatens-to-send-Hitman-unless-ransom-amount-in-the-form-of-Bitcoin-is-paid.htm> accessed 11 July 2022
- White house government, ‘Executive Order on Ensuring Responsible Development of Digital Assets’ (*White House* , 9 March 2022) <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/> accessed 3 September 2022
- Wikipedia, 'Crisis Financiera de 2008 ' (*Wikipedia,* 1 June 2022) <https://es.wikipedia.org/wiki/Crisis_financiera_de_2008> accessed 1 June 2022.
- “China Primer: Illicit Fentanyl and China’s Role - Congress” <https://crsreports.congress.gov/product/pdf/IF/IF10890> accessed December 2, 2022
- “Great Firewall” (WikipediaNovember 26, 2022) <https://en.wikipedia.org/wiki/Great_Firewall> accessed December 2, 2022
- “Two Chinese Nationals Charged with Laundering over $100 Million in Cryptocurrency from Exchange Hack” (The United States Department of JusticeJuly 22, 2022) <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack> accessed December 2, 2022
- About the authors: Kurt Woock is a writer at NerdWallet. Read moreAndy Rosen is a NerdWallet writer focused on cryptocurrency and alternative investments. He has more than 15 years of journalism experience as a reporter and editor at organizations includ, “Crypto Taxes in 2022: Tax Rules for Bitcoin and Others” (*NerdWallet*)

<https://www.nerdwallet.com/article/investing/bitcoin-taxes> accessed November 19, 2022

- "A Brief History of Cryptocurrency Regulation in the US" (*Web3Caff*) <https://web3caff.com/archives/15720> accessed November 17, 2022
- Esparragoza L, "Hace 10 Años Nació Silk Road, Primer Mercado De La Dark Web Que Aceptó Bitcoin" (*CriptoNoticias*January 30, 2021) <https://www.criptonoticias.com/comunidad/10-anos-nacio-silk-road-primer-mercado-darkweb-acepto-bitcoin/> accessed December 2, 2022
- "Executive Order on Ensuring Responsible Development of Digital Assets" (*The White House*March 9, 2022) <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/> accessed November 21, 2022
- "Ice Statement for the Record for a Senate Committee on Homeland Security and Governmental Affairs Hearing Titled 'Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies'" (*ICE statement for the record for a Senate Committee on Homeland Security and Governmental Affairs hearing titled "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies" | Homeland Security*) <https://www.dhs.gov/news/2013/11/18/ice-statement-record-senate-committee-homeland-security-and-governmental-affairs> accessed November 17, 2022
- Martínez J, "España Es El Quinto País De Europa Con Mayor Volumen De Transacciones En Criptomonedas" (*BeInCrypto*April 27, 2022) <https://es.beincrypto.com/espana-quinto-pais-europa-mayor-volumen-transacciones-criptomonedas/> accessed December 2, 2022
- Ministerie van Justitie en Veiligheid, "Fiod En Om Leggen Beslag Op Meer Dan 25 Miljoen Euro Aan Cryptovaluta in Witwasonderzoek" (*Nieuwsbericht | Openbaar Ministerie*November 8, 2021) <https://www.om.nl/actueel/nieuws/2021/11/08/fiod-en-om-leggen-beslag-op-meer-dan-25-miljoen-euro-aan-cryptovaluta-in-witwasonderzoek> accessed November 16, 2022
- Olatunji T, "Are Cryptocurrencies Securities? The Howey Test and Its Implications" (*MUO*November 14, 2022) <https://www.makeuseof.com/are-cryptocurrencies-securities/> accessed November 20, 2022
- Person R and Chavez-Dreyfuss G, "Chinese Crypto Addresses Sent $2.2 Bln to Scams, Darknets in 2019-2021 -Report" (*Reuters*August 3, 2021)

<https://www.reuters.com/technology/chinese-crypto-addresses-sent-22-bln-scams-darknets-2019-2021-report-2021-08-03/> accessed December 2, 2022

- Person, "China Bans Financial, Payment Institutions from Cryptocurrency Business" (*Reuters*May 18, 2021) <https://www.reuters.com/technology/chinese-financial-payment-bodies-barred-cryptocurrency-business-2021-05-18/> accessed December 2, 2022
- "The Rules for Anti-Money Laundering by Financial Institutions" (*The rules for anti-money laundering by financial institutions*) <http://english.www.gov.cn/services/investment/2014/08/23/content_281474982978019.htm> accessed December 2, 2022
- Times G, "Over 90% of Crypto-Related Businesses Shut down in China after Ban" (*Global Times*) <https://www.globaltimes.cn/page/202110/1235801.shtml> accessed December 2, 2022
- Winnowicz K, Au C-D and Stein D, "Crypto Regulation within the European Union" (*SSRN*August 26, 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4194771> accessed November 2, 2022
- Zolciak A, "A Look at EU's GDPR and What It Means for Crypto Privacy" (*CoinDesk Latest Headlines RSS*November 7, 2022) <https://www.coindesk.com/layer2/privacyweek/2022/01/28/a-look-at-eus-gdpr-and-what-it-means-for-crypto-privacy/> accessed November 3, 2022
- Winnowicz K, Au C, and Stein D, 'Regulation of Cryptocurrencies in the European Union – Impact of the European Regulatory Notifications on the cryptocurrency market' (4th International Conference on Applied Research in Business, Management and Economics, Prague, 2022) < https://www.researchgate.net/publication/359391758_Regulation_of_Cryptocurrencies_in_the_European_Union_-Impact_of_European_regulatory_notifications_on_the_cryptocurrency_market > Accessed 27 August 2022
- Almarcha Navidad C, 'Bitcoin, Oro Electrónico' (Degree Final Dissertation, Universidad de Ciencias Sociales y Jurídicas de Elche, 2015)
- Bartolomeo A, Machin U. G, 'Introducción a la Tecnología Blockchain: Su impacto en las ciencias económicas' (Dissertation, N/D).
- Gisin Nicolas and others, 'Quantum cryptography' [2022] 74(145) APS Physics

- Global legal insight , 'Blockchain and Cryptocurrency Laws and Regulations 2023 Hong Kong ' (GLI , 2023) <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/hong-kong> accessed 13 May 2023
- I.L. Márquez-Legajo T, 'Bitcoin, un análisis de los determinantes de su valor en Argentina' (Master's Final Dissertation, Universidad de San Andrés, 2018)
- Largo Suarez V, 'La fiscalidad de las criptomonedas en España = Taxation of cryptocurrencies in Spain, (Degree Final Dissertation, Universidad de León, 2019)
- Noriega Poletti S.P 'Regulación de las Criptomonedas para garantía de sus beneficios) Degree Final Dissertation, Universidad de los Andes, 2018)