LUISS

Dipartimento di Scienze Politiche

Corso di laurea magistrale in Relazioni Internazionali

Cattedra di Geografia Politica

The impact and geopolitical consequences of sanctions evasion through cryptocurrencies

Prof. Alfonso Giordano
RELATORE

Prof. Paolo Garonna
CORRELATORE

Angelo Tozzi
Matr. 640222
CANDIDATO

Anno Accademico 2020/2021

RINGRAZIAMENTI

Ringrazio il Professor Alfonso Giordano, per i suoi preziosi consigli e la sua costante disponibilità nel corso della realizzazione di questo lavoro conclusivo.

Ringrazio il Professor Paolo Garonna, per la sua disponibilità e la sua supervisione nel corso della stesura dell'elaborato.

Ringrazio il Professor Francesco Giumelli, per avermi dato l'opportunità di lavorare ed approfondire un tema poco conosciuto ma, allo stesso tempo, molto stimolante ed intrigante.

Ringrazio tutta la mia famiglia, perché, grazie ai loro sforzi, mi hanno permesso di intraprendere questo percorso, sostenendomi sempre e non facendomi mai mancare il loro affetto ed il loro pensiero. La fiducia riposta in me ha rappresentato un grande stimolo per raggiungere questo traguardo.

Ringrazio i miei amici, quelli di sempre, che ho ancora il piacere e la fortuna di avere accanto e quelli incontrati lungo la strada della vita, perché, spesso, più che la quantità, è la qualità del tempo ad avere un'importanza maggiore, mantenerla non è una sfida semplice, riempirla di valori è ancora più gratificante.

Ringrazio i miei colleghi, fedeli compagni di viaggio lungo un percorso travagliato ed insolito, viste le particolari modalità con le quali è passato. La tenacia nel rimanere uniti, farsi forza vicendevolmente e scambiarsi preziosi consigli ha avuto un ruolo prezioso in questo cammino.

Encourage, lift and strengthen one another.

For the positive energy spread to one will be felt by us all.

For we are connected, one and all.

TABLE OF CONTENTS

LIST OF FIGURES **7**
LIST OF BOXES **7**
LIST OF TABLES **7**
INTRODUCTION **9**
Chapter 1 ..... **15**
Mapping an invisible boundary: the geopolitics of digital space **15**
1.1 Cyberspace: early studies, evolution and affirmation 15
1.2 The geography of cyberspace 19
1.3 How cyberspace affects geopolitics and international relations 25
1.4 Use of cyberspace by Islamic terrorism 29
1.5 The desire for sovereignty: independence in cyberspace 33
Chapter 2 ..... **36**
The instrument of sanctions **36**
2.1 UN legislation and its sanctions system 36
2.2 Different types of sanctions: a historical analysis of the instrument and the evolution of its use before and after the cold war 42
2.2.1 Apartheid South Africa 44
2.2.2 Southern Rhodesia 50
2.2.3 The end of cold war and the beginning of a new era: from comprehensive to targeted sanctions 54
2.3 European Union sanctions 60
2.3.1 The decision-making process 61
2.3.2 The role of Common Foreign and Security Policy (CFSP) in imposing sanctions 63
2.3.3 Case Study: European Union v. Belarus 65
2.4 The geopolitical meaning of energy sanctions 69
2.4.1 Case study: US v. Iran 74
2.4.2 Latest development: the Joint Comprehensive Plan of Action (JCPOA) and the two new presidencies: what are the possible scenarios? 76
Chapter 3 ..... **82**
Cryptocurrencies: understanding the phenomenon and its evolution **82**
3.1 Origin of a digital currency and its working principles 82
3.1.1 Blockchain 87
3.1.2 Smart contracts 92
3.1.3 The impact of cryptocurrency mining 95
3.2 Evolution and growth of the cryptomarket 98

3.3 The governance of cryptocurrencies 100
3.3.1 Blockchain technologies: a double governance 102
3.4 Crypto-regulation: the position of international organizations and possible future development 105
Chapter 4 112
The geopolitics of cryptocurrencies 112
4.1 What is the geopolitical influence of cryptocurrencies? 112
4.2 How the attitude of the world's governments has changed in relation to the growth of cryptocurrencies 113
4.2.1 China's case 115
4.2.2 Venezuela's case 120
4.2.3 San Salvador's case 123
4.3 Shaping the future: are cryptocurrencies the money of the future? 126
4.3.1 Opportunities and advantages 127
4.3.2 Risks and threats 129
4.3.3 Possible improvements 131
Chapter 5 135
How cryptocurrencies are used to escape from sanctions 135
5.1 The phenomenon of sanctions evasion 135
5.2 European Union and United States crypto-regime 137
5.3 Actors: who escapes, how and why? A geopolitical bond 142
5.4 How to steam the illicit 150
CONCLUSIONS 155
REFERENCES 158
ABSTRACT 170

LIST OF FIGURES

Figure 1.1 – *Visualizing different aspects of cyberspace*

Figure 1.2 – *TeleGeography's Submarine Cable Map (August 2021).*

Figure 1.3 – *Global Public Cloud Revenue*

Figure 1.4 - *IaaS & SaaS, 2019 Public Cloud Market Share*

Figure 1.5 – *Independence in cyberspace*

Figure 2.1 – *The governance structure of security council sanctions regime*

Figure 2.2 – *Values of trade during the sanctions period in Apartheid South Africa*

Figure 3.1 – *First Bitcoin transaction*

Figure 3.2 – *Type of systems*

Figure 3.3 – *Cryptographic hash function*

Figure 3.4 – *P2P network of blockchain*

Figure 3.5 – *Different smart contracts applications*

Figure 4.1 – *Impact of remittances in dollars and in relation to GDP*

Figure 4.2 – *Compared breakdown by region: interest in three main cryptocurrencies (period 2008-present)*

Figure 4.3 – *Reasons for not supporting a new cryptocurrency*

Figure 5.1 – *SWIFT evolution over time*

Figure 5.2 – *WannaCry attack process*

Figure 5.3 – *Iran's Share of Bitcoin Mining*

LIST OF BOXES

Box 2.1 – *UN Charter – Article 39 and Article 103*

Box 2.2 – *Trygve Lie Appraises the Future of the U.N. – New York Times 9 May 1948*

LIST OF TABLES

Table 2.1 – *Use of veto by permanent five member states*

Table 2.2 – Distinctive features of targeted sanctions: objectives and targets

Table 2.3 – *Effectiveness by purpose and type of direct impacts*

Table 2.4 – *Procedure for approval and implementation of sanctions-related CFSP decision*

Table 3.1 – *Mortality impacts, climate damages, and health damages of coin mining created by country, year and cryptocurrency*

Table 4.1 – *Nationality of mining pools and their share of hash rate between May 1st, 2015 and June 30, 2016*

Table 4.2 – *A summary of five Deep Web marketplaces*

INTRODUCTION

The final work aims to go deeper and analyse the evasion of sanctions through cryptocurrencies, trying to explain the impacts and consequences of this phenomenon also under the geopolitical aspect. In order to answer the question of how sanctions are evaded through this instrument, it was necessary to proceed by studying the various elements involved: cyberspace, sanctions and cryptocurrencies. The idea stems from the desire to find out about new ways of stopping illegal activity through the use of this phenomenon, through cutting-edge technology and computing power, first of all, laying bare the risks inherent in the cryptocurrencies themselves, and then trying to assess the possible developments and changes to ensure that there are also positive implications in terms of combating illegal activity. To develop an interdisciplinary work, which therefore presents various topics unrelated to each other but united by the central theme and the intention to answer the research question, a thorough examination of the existing literature is very useful, to understand the reason for their emergence, their evolution, their effects and their current use.

For the analysis of cyberspace, the intention has been to study the birth and emergence of this new dimension, the related theories and the authors who have expressed them. The phenomenon in question, which is the central subject of the concluding work, cannot in fact disregard the geo-spatial aspect. Geo-space is obviously linked to geopolitical factors and influences international relations, given its growing importance and use across the world. Through the study of maps, we tried to visualize and deepen various characteristics present within cyberspace, understand its internal geography, how the world is increasingly connected and understand the mechanism that allows this connection. Analyzing this last aspect, one notes the importance also of the ownership of these connections and of guaranteeing the security and privacy of an ever-increasing number of users. The continuous increase of social dependence on ICTs at all levels has consequently changed the way in which individuals interact both professionally and personally. The role of technology has changed the way society is interpreted and how it has influenced power relations. Cyberspace has, in fact, activated a series of social, economic and political problems, having the capacity to shift these problems from the local and internal level to the international level, creating the need for cooperation within cyberspace by different actors, especially with regard to the security of individuals' data. It was precisely in response to these fears and insecurities that ICANN (Internet Corporation for Assigned Names and Numbers) was born[1].

The institution of sanctions is frequently used by large international organisations and an analysis of their geopolitical value is of absolute importance. The instrument has been extensively studied and deepened, with a particular emphasis on the action of different actors: United Nations, European Union and United States. In

[1] Radu, R. (2014). Power technology and powerful technologies: global governmentality and security in the cyberspace. In *Cyberspace and International Relations* (pp. 3-20). Springer, Berlin, Heidelberg.

order to do so, several sources have been used to analyse in detail the evolution of the instrument, initially conceived as an instrument of war and then transformed into an instrument of peace; the governance present in order to decide and implement sanctions and, finally, several scholars have analysed case studies in order to assess the effectiveness and efficiency of sanctions.

As is well known, the discipline of sanctions has changed profoundly since before the United Nations Charter came into force. The distinctive character of sanctions in the technical sense in contemporary international law is, in fact, their institutionalisation: that is, the fact that they are collective measures decided or recommended by international organisations[2]. At the same time, sanctions, over time, have increasingly assumed a value and implication also at the geopolitical level. The instrument is used both to emphasise - and widen - the divergences between two states or between an international organisation and another state, and as a countermeasure with events in contrast with the values of one organisation (state or international) carried out by another entity, the most recent example being the sanctions imposed by the European Union on Belarus following the hijacking of an aeroplane to arrest dissident Raman Protasevich. The connection with the geopolitics of sanctions is also punctual to the numerous variables that this instrument presents: the temporal dimension, the modality, the reason and, certainly, the spatial dimension should not be underestimated. Additionally, the forms of sanctions as well as the reasons that led to the imposition of them have changed over time. If arms embargoes were the most common type of sanctions in the first-decade post-Maastricht, asset freezes, and travel bans would become the most prevalent forms in the last 15 years. Similarly, while one main pattern could not be identified in the first years after 1993, it eventually became clear that democracy promotion was the most frequent reason for the EU resorting to sanctions. Conversely, the geographical distribution of sanctions has not changed over time, with the EU imposing restrictive measures both in its immediate vicinity and elsewhere[3]. If on one side, there are several academic contributions to the instrument of sanctions, and just as many concerning geopolitics in general, on the other side there is a lack of literature combining these two themes. The aim, therefore, is to bring together, through specific case studies, both more or less recent, sanctions and geopolitics, to deepen the links between these two closely related topics, to achieve a more coherent and linear contribution to explaining the evolution that occurs and changes in relations between states and/or international organisations.

Despite the growing popularity of cryptocurrencies, their use is far from being fully known. Every discovery and every alternative way of modifying everyday life brings with it both positive aspects and shadows with

[2] Silingardi, S. (2020). *Le sanzioni unilaterali e le sanzioni con applicazione extraterritoriale nel diritto internazionale*. Giuffrè Francis Lefebvre.

[3] Giumelli, F., Hoffmann, F., & Książczaková, A. (2021). The when, what, where and why of European Union sanctions. *European Security*, *30*(1), 1-23.

gaps that need to be filled to prevent them from being exploited by criminal and harmful entities. Interestingly, the combination of quasi-anonymity and the decentralised nature of cryptocurrencies has relevant reflections concerning anti-money laundering efforts to be implemented[4]. In this sense, the aim is to study how sanctions are evaded and circumvented through the instrument of cryptocurrencies and to explore the implications of these.

Regarding the descriptive character of the project, there are, as mentioned, several topics that will be analysed. Each subject will be deepened by focusing more on one aspect rather than another, obviously leaving aside those which will be external parameters, that is, aspects that will be taken for granted or not susceptible to analysis and study because they are too distinct and not strictly coherent with the central question. In this sense, the core of the work will concern, as already mentioned, the evasion of sanctions and the various applications of cryptocurrencies and blockchain technologies. Consequently, topics and issues such as the volatility of cryptocurrencies, economic implications and how they are created will be marginally or absent. On the other hand, of absolute relevance will be the so-called internal mechanisms, i.e., what is considered as a problem and will be the object of study: the evasion of sanctions through cryptocurrencies. The variables present and the sequence that occurs to achieve this evasion but, above all, the causal links that exist are themes of primary importance in the work. Once this dynamic has been deepened, with all the points of question and the various operative modalities that, inevitably, the object of the study brings with it, an analysis of the role of governments and international organisations in the fight against the evasion of sanctions through cryptocurrencies is equally important. Many governments have taken a neutral or negative stance on the issue of cryptocurrencies. Some governments have even banned Bitcoin altogether. Large companies are not openly willing to step up and invest in Bitcoin and related technologies. Despite all this, Ethereum (another Bitcoin-like cryptocurrency with advanced features) has emerged. Today there are several cryptocurrencies on the market. But it seems that Bitcoin has found a successor in Ethereum. In the wake of the activities carried out by the international organisations, the role of the national governments and the perimeter within which they operate is equally stimulating. What action can they take? Some states have banned cryptocurrency transactions and conversions, as well as cryptocurrency-related activities; others have tried, with varying degrees of success, to ban cryptocurrency mining; and still, other states have tried to exploit cryptocurrencies to get out of dire economic situations, even going so far as to create a state-run cryptocurrency. The impression, after an initial assessment, seems to be that of entering a parallel world with boundless possibilities but also freedom, which is the most trivial consequence of deregulation, that needs to be limited to avoid the proliferation of the illicit in the broadest sense. Sanctions have become a popular tool of other multilateral institutions – most notably the European Union – and we have seen innovative use of unilateral sanctions by

[4] Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law, and Social Change, 69*(2), 283-305. https://doi.org/10.1007/s10611-017-9756-5

states in a broad range of circumstances. It was inevitable that this increased activity in the use of measures that affect economies, industry, financial services and individual rights would generate complex legal issues and challenges[5]. On the one hand, governments and large companies are wary of cryptocurrencies. On the other hand, some companies are secretly rushing ahead to build their blockchain network and infrastructure. This situation will only lead to more and more unregulated and unknown elements entering the cryptocurrency fray. By the time governments react, it may be too late. Governance and geopolitics are closely intertwined. Taking a different perspective, it should be noted that cryptocurrencies are being harnessed by several governments seeking to circumvent international sanctions regimes imposed by the United Nations, the United States and the European Union. At the same time, and in response to the advent of sanctions-evasion schemes utilizing cryptocurrencies, the US has enhanced sanctions against Iranian actors while the EU has elaborated restrictive measures targeting financial crimes carried out with cryptocurrencies[6]. In any case, as already stated, the aim of this work is to know and investigate the negative and obscure aspects, as well as the regulatory gaps, in relation to the use of cryptocurrencies but, at the same time, to offer a proposal that could be positive and virtuous for the community. In this sense, it is well-known that blockchain has the potential to be a game-changer in anti-corruption efforts. Whether it is successful or not largely depends on contextual elements – infrastructures, legal systems, social or political settings – rather than on the technology itself. Blockchain technologies are attracting development organisations and anti-corruption communities because of their potential to prevent corruption and protect public registries from fraud and tampering. The success and failure of blockchain-based projects depend on the surrounding infrastructure and the social or political context rather than on the technology itself. Still, in its early days, blockchain technologies lack stringent standards and an agreed-upon terminology. Decision-makers should therefore fully understand this emerging technology to gauge its applicability in different contexts. Particularly in developing countries, it is important to understand if the prerequisites of connectivity, digitised data, and digital literacy exists before launching blockchain-based projects[7]. Like Aarvik, Campbell-Verduyn also supports a possible virtuous and positive vision of cryptocurrencies. In his paper "bitcoin, crypto-coins, and global anti-money laundering governance", he argues that cryptocurrencies, if properly managed, will greatly simplify people's governance and lifestyles, increase people's access to resources and services, and ultimately usher in an egalitarian world order where nationally and internationally all people will be more or less equal.

---

[5] Gordon, R., Smyth, M., & Cornell, T. (2019). *Sanctions Law*. Bloomsbury Publishing.

[6] Giumelli, F. (2021). Cryptocurrencies, Blockchain Technologies and International Sanctions: Towards New or Old Financial/Security Infrastuctures? , viewed on 29/06/21 https://www.giumelli.org/projects/cryptocurrencies-blockchain-technologies-and-sanctions .

[7] Aarvik, P. (2020). Blockchain as an anti-corruption tool: Case examples and introduction to the technology. *U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute (U4 Issue 2020: 7)*.

However, the project intends to develop through multiple selections of case studies and historical-political analysis, both regarding sanctions and their geopolitical implications, and regarding the various behaviours adopted by national governments and international organisations in response to the growth of cryptocurrencies, with all the problems and gaps to be filled that this growth, as already explained, may bring with it. In both cases, of primary importance will be the instrument of comparison, useful to analyse the differences between the various cases selected. There will therefore be several units of observation, belonging, of course, to a single sample. For instance, it will certainly be interesting to analyse the recent sanctions imposed by the European Union against Belarus, delving into the process also at a legislative level and understanding the geopolitical consequences of the affair. To proceed in a coherent reasoning, it will be necessary to analyse also how the instrument has evolved in the European Union, comparing, therefore, this last countermeasure with others already adopted in the past against other States, to try to arrive at a conclusion which can answer the most classic of the questions on this instrument: are the sanctions effective? At the same time, in the examination of the behaviour of national governments about the emergence of cryptocurrencies, several case studies will be present, many of which are recent and current. To understand the reasons, it will certainly be useful to delve into the economic panorama, but it is not to underestimate the geopolitical aspect of the States examined, many of which are grappling with both high rates of inflation and with - often - stormy relations with the United States and, in general, with the great world financial institutions. With Washington, the reason for the fragility of relations is both geographical proximity and the weakness of the currency, which needs the support of the dollar. On the other hand, relations with institutions such as the International Monetary Fund or the World Bank are also delicate, given the amount of debt that these developing countries hold.

Chapter 1

Mapping an invisible boundary: the geopolitics of digital space

1.1 Cyberspace: early studies, evolution and affirmation

The term cyberspace is increasingly used in our information technology age. It was initially coined by Gibson in his well-known science fiction novel Neuromancer. Cyberspace is defined as a computer-generated landscape, i.e., the virtual space of a global computer network, linking all people, computers, and sources of various information in the world through which one could navigate. It has become a more and more dominant aspect of our society. Cartography, hitherto regarded as a discipline for mapping the real world, is experiencing a big challenge to map cyberspace. Most cartographic principles can also be used for mapping cyberspace. Various cybermaps have been discussed regarding their uses for navigation, analysis and persuasion. However, cyberspace is rather different from the real world we live in. For example, the Earth is an irregular sphere, and mapping it requires flattening it to a two-dimensional plane, for which direction, distance, area and scale are critical factors. For cyberspace no such simple model as the globe exists. Instead, various different models of virtual space can be constructed. These differences provide a big challenge for mapping virtual worlds. Traditional cartography is based on Euclidean geometry because the correct representation of distances and directions is an important concern in such activities as navigation, exploration and land management. This traditional focus has already been changed somehow since the 1930s by the emergence of topology and topological mapping. Here, the primary concern was not to render areas or object categories, but to focus on connectivity, i.e., on the fact of whether or not locations (nodes) have been linked. The importance of the distance factor is decreasing due to the development of telecommunications and because of the Internet as an information dissemination support. Instead of distance it is relations that become increasingly important for understanding network structures. This change causes many differences between cybermaps and traditional maps. However, there are many similarities between cyberspace and geographic space; for example, both are too large to perceive in their entirety. It is possible to orient the discussion towards three categories of cybermaps. A distinction is made first between three views of cyberspace that can be discerned: the first which considers cyberspace as a set of physical anchorages, the second which concentrates on the topological relationships and the third which regards cyberspace as an animated 3D computer-based model. Thus, the first view leads to cybermaps with representations of the Earth as a base map; the second view leads to maps of topological relationships and the third produces general purpose maps for virtual worlds. As opposed to direction and distance, it is connectivity and integration of topology that appear to be critical in mapping cyberspace. Space is probably one of the most essential and paradoxical concepts that human beings face. Space is always present in our everyday life, for instance, travelling all over the world, being in a country, a

city, even in a building. Basically, two kinds of space can be identified in terms of size of space from the point of view of perception: small space which can be seen from a single viewpoint and large space which is beyond human body perception and cannot be seen from a single vantage point. To understand and perceive large space, maps are often used to represent it on a small-scale paper plane. In other words, we need maps because space is too large to perceive, to understand, to navigate and to explore. Maps provide a visualization tool for understanding and perception of space. So, traditional cartography is defined as `the art, science and technology of making maps, together with their study as scientific documents and works of art. In this context, maps may be regarded as including all types of maps, plans, charts and sections, three-dimensional models and globes representing the earth or any celestial body at any scale'. In this definition, both cartographies, as a discipline for mapping and maps is defined in rather restrictive terms. Two points deserve mention here. The first is that maps were initially meant for portraying the Earth or parts of the Earth and were developed later on for any celestial body. This constraint does not remain valid, as the notion of maps has been widely used for mapping brain or other micro-organs. The second concern about the above definition is scale. Scale always comes with size; for instance, we need to represent a country or a city at a reduced scale in order to fit a paper sheet. This may not be completely true for cyberspace. Cyberspace is large in the sense of its physical extent. On the other hand, it is small in the sense that distance in cyberspace is non-existent. Through telepresence, people can be `together' despite geographical and/or temporal distance. When we state that cyberspace is small, it does not mean that we do not need a map for it. On the contrary, we need a map for it as its structure has become very complex so that it cannot be perceived in its entirety. Cyberspace maintains many differences from geographic or physical space. Firstly, for the Internet, it can be regarded as both an information infrastructure attached to the Earth and as information networks without any distance concept. Secondly, developed from the virtual reality technique, 3D computer-based models with or without Internet connection constitute another sort of cyberspace within which one can walk through or fly over with a mouse or special headset. From the traditional classification of maps into general reference maps and special purpose maps, it seems that the information infrastructure view of the Internet leads to cybermaps being classified as thematic maps. In this connection, many traditional thematic cartographic principles can be used in mapping this kind of cyberspace. The information networks view of the Internet leads to network mapping, which has similar cartographic fundamentals. In Bertin's Semiology of Graphics (1983), one chapter has been contributed to the issue. Nowadays, it is considered quite acceptable to make available to the general public various schematic maps such as subway networks, the urban bus network and suburban railroad network. Travellers are also accustomed to exposure to documents showing the airline networks. In these schematic maps, real location and metric distance become less important compared to the topological relationships. Thinking about sitemaps, represented as a topological structure, each node has no meaning whatsoever in terms of physical location, neither has a link any physical meaning other than that of showing a relationship. The Internet is a world-wide network of millions of computers communicating via an agreed upon set of Internet protocols. Because so

many computers are networked together, the analogy `information superhighway' is often used. Physically speaking, all computers have their unique location on the Earth. Therefore, the Internet can be regarded as a space attached to the Earth. Thus, mapping Internet space would be mapping physical locations of computers distributed all over the World. This kind of cybermap can be thought of as a thematic map with a topographic map for a base map. Its mapping procedure follows the principle of traditional thematic mapping. In this connection, MIDS (1999) provides a huge amount of sample maps for the Internet.

These cybermaps can be categorized according to themes as follows:

- Internet growth (rate),
- Internet weather forecast
- Domain Name System (DNS)
- distribution of hosts, and nformation volume etc.

Over the Internet, it is web servers that maintain detailed logs of every request made for information. Here every request is referred to as a hit. The number of hits reflects the frequency of usage of a specific web site. Both the number and distribution of hits can be mapped. When using the visual variables proposed by Bertin (1983), the various domains (.gov, .edu, .com) could be differentiated through the use of colours, and hosts and domains through differences in shape. Figure 1 suggests a set of visualizations used in mapping cyberspace, with the Earth as a flat plane. Actually, it should be more realistically represented as part of globe. Mapping location, distribution and volume of the Internet according to geography is a major task for cyberspace. Various efforts have been made towards visualizing the Internet in three dimensional and dynamic ways, which provide more intuitive communication and analytical tools for the Internet. In contrast to the Internet, the Intranet, though based on the same technology, is restricted to relations within an organization or enterprise. Except for the size of cyberspace, the Internet and Intranet have no differences. The Intranet, however, can be regarded as a subset of the Internet[8].

[8] Jiang, B., & Ormeling, F. (2000). Mapping cyberspace: Visualizing, analysing and exploring virtual worlds. *The Cartographic Journal*, Volume *37*, Issue 2, 117-122.

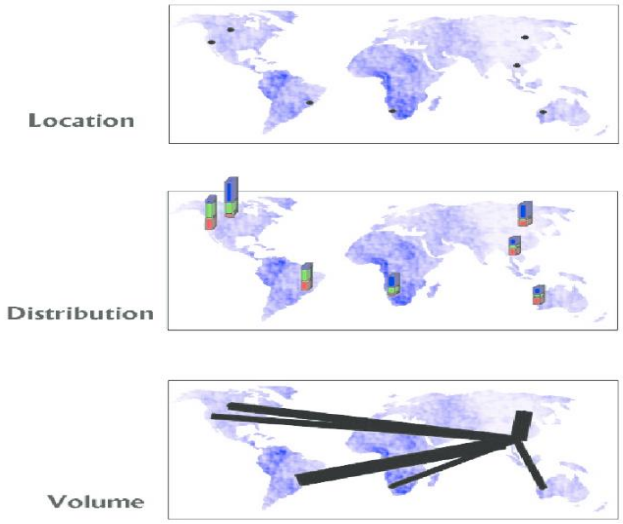


Figure 1.1 – Visualizing different aspects of cyberspace

Source: Jiang, B., & Ormeling, F. (2000). Mapping cyberspace: Visualizing, analysing and exploring virtual worlds. *The Cartographic Journal*, Volume *37*, Issue 2, 117-122.

Cyberspace is a social space in which people can meet under new definitions of encounter and personalisation. The collapse of spatio-temporal relations and the evolution of new space-less and place-fewer social spaces (Facebook, LinkedIn, Twitter, MySpace) call into question the importance of geographical places to such an extent that some are convinced that geography and time are no longer boundaries. Cyberspace is profoundly anti-spatial, since you cannot tell where it is, and you cannot describe its shape and size. You can find things in cyberspace without knowing where they are! In a way, the despatialisation brought about by the Internet destroys the key of the 'geocode'. Conversely, this new form of communication depends on spatial links in the real world, on the geographical location of access points, on the materiality of fibre optic cables, on WiFi - in the absence of cables and telephone wires. If Internet access is of excellent quality in one place, while it is absent in another place, this is another proof of the importance of geographical position and location. The technologies of cyberspace can accentuate differences or emphasise competition between geographical locations, making it possible to access places with the lowest wages or the best services. The new economic geography comes to the same conclusion about the role of cyberspace in firms' location strategies. In many cases, cyberspace favours concentration tendencies by virtue of its connection to telecommunications infrastructures and the social environment of large metropolises. Similarly, services that can be decentralised are more likely to be in regions with an adequate workforce and good transport conditions. New communication technologies make it easier for large industrial companies (Colgate, Google, McDonald's, Coca Cola) to pursue their global strategies, but consumers do not make their purchases according to a global strategy. They only want the best products and services in the area they know best, nearby. Google suffers from state censorship in China and faces strict privacy legislation in Germany. Suddenly, Google - whose

product has no physical form - has found itself anchored to geographical locations. The Internet and the mobile phone have transformed marketing processes, lowering the physical barriers of places. But, as the example of Google in China and Germany demonstrates, geography still matters in in practice, even if cyberspace markets are theoretically exempt from the borders of conventional borders of conventional geographies. In fact, the political frontiers associated laws, regulations, taxes and trade agreements govern sellers and their physical or digital products. Relatively few online transactions cross national borders. The idea of the end of geography focuses on the levelling effects of the third globalisation, while the idea of the revenge of geography accepts the point of view of the spatial differences present in local, regional and national contexts. These two tendencies (levelling and differentiation) substantiate a dialectic that is permanent in national economies. It is the task of geographers to draw the public's attention to the existence of these two ideas and to declare that geography is always important, albeit in different ways[9].

1.2 The geography of cyberspace

The advent of cyberspace has not erased geography, it has reconfigured it. A prominent role is, in fact, played by the submarine cables that trace the main naval trade routes and routes and form the backbone of the Internet. Along these arteries, large providers of data storage, retention and processing services are located. But what happens when not only the infrastructure through which 99% of data passes and is stored, but also the content through which that data is generated, is in the hands of a single actor? Almost all global Internet traffic is carried by sea through undersea fibre-optic cables. To be precise, 99% of the data exchanged in the world, making undersea cables the backbone of the global internet and the backbone of the globalised economy. Planetary connections rely on these infrastructures for their efficiency and cost-effectiveness. cheaper than satellites, are often transnational in nature and have transnational character and have a high capacity in terms of terabytes. While the vehicle for global connections is undersea cables, the main physical main physical locations for storing, sharing and processing transmitted data are data centres and, in particular, cloud service providers. These are private companies that manage the data of billions of users (public and private) on a global scale. When cloud service providers are also content providers like content providers such as Google, Amazon and Microsoft, it is the digital sovereignty of the states that is threatened, or at least there is a power disparity in the management of critical infrastructures. critical infrastructure. Submarine fibre-optic cables have been connecting countries and continents since the 1980s. In 1988, the first cable was laid, the TAT-8 was laid in 1988, connecting the US, the UK and France. Since then, it is estimated that the undersea fibre-

[9] Sanguin, A. L. (2014). Fine della geografia o rivincita della geografia. *Le societa umane in un mondo liscio, un mondo „puntuto" o un mondo piatto//Bollettino della Societa Geografica Italiana. Serie XIII*, *7*, 445-460

optic network has grown too about approximately 400 cables worldwide. Looking at their geographical distribution, these cables follow the main shipping routes: from the coasts of the United States, the most connected country in the world, they propagate several cable routes run towards Europe and the Indo-Pacific region. The Mediterranean Sea is also very busy, with numerous cables entering the Red Sea and reaching the Far East and South-East Asia via the Indian Ocean. The route of a cable does not usually comprise a single point of arrival, but multiple 'landing points': cables often branch out in multiple directions to connect multiple locations simultaneously. There are cables of high strategic importance that connect several continents, such as SeaMeWe-3, the world's longest cable at 39,000 km. SeaMeWe-3 connects Europe to the Far East and Australia via the Indian Ocean, connecting a total of 38 cities. The development of undersea cabling is mainly driven by private investment rather than by state will: companies choose the most important routes, those that connect the main catchment areas. For this reason, in recent years the region with the most investment in this sector has also been the one with the highest population growth rate, namely the Indo-Pacific region. Today, these cables are mostly owned by consortia of private companies: a single cable is owned by all the companies that contributed to its design and construction. The companies are often of the same nationality as the countries benefiting from the connection brought by the cable, but they can also be international companies investing in areas other than their own country, such as the American company AT&T or the Indian company TATA Communications. Such is the importance of these cables that even the American Big Techs have started to design and own their own submarine cables: Google, Facebook, Amazon and Microsoft have recently started to lay their own cables, of which they are partial or in some cases sole owners. This is the case with Google, which owns the Curie (United States-Panama-Chile), Dunant (United States-France) and Junior (Brazil) cables. Despite their importance, these cables are essentially vulnerable. They are around 25m in size and are exposed to numerous risks, from natural disasters to ship anchors and deliberate human damage. In March 2013, the Egyptian coastguard caught three divers cutting a cable off the coast of Alexandria. Although the divers' motivation was not made public, the event demonstrated how precarious and important this infrastructure is.

Therefore, in addition to planning and maintenance, it is important to be able to rely on an extensive cable network, so that the extent of any damage can be minimised. Damage to a cable could disrupt the flow of data, but even the mere slowing of the flow of data could be fatal to financial operations and military communications, especially in times of crisis and conflict. The economic and strategic importance of these cables has often placed them at the centre of geopolitical disputes involving companies and governments. A case in point is the Pacific Light Cable Network (PLCN). designed by Facebook and Google in 2016 to connect the US, the Philippines, Taiwan and Hong Kong. The project was opposed by the US government in 2020, as the Los Angeles-Hong Kong route was considered risky because the Chinese government could have a channel to access US data, especially since the autonomy of the special-status city has been called into question by recent events. The effort of governments is therefore to be able companies to protect

national security and avoid projects that could potentially potentially expose their data to external threats. Another strategic objective concerns the differentiation of their cable network, having multiple routes so as not to depend on the connections that cross a given country. Brazil, for example, will have EllaLink in 2021, a cable that connects the country directly to Europe, with the implicit aim of providing access to the old continent's network without going through US cables, on which Latin America is largely dependent for intercontinental connections[10].

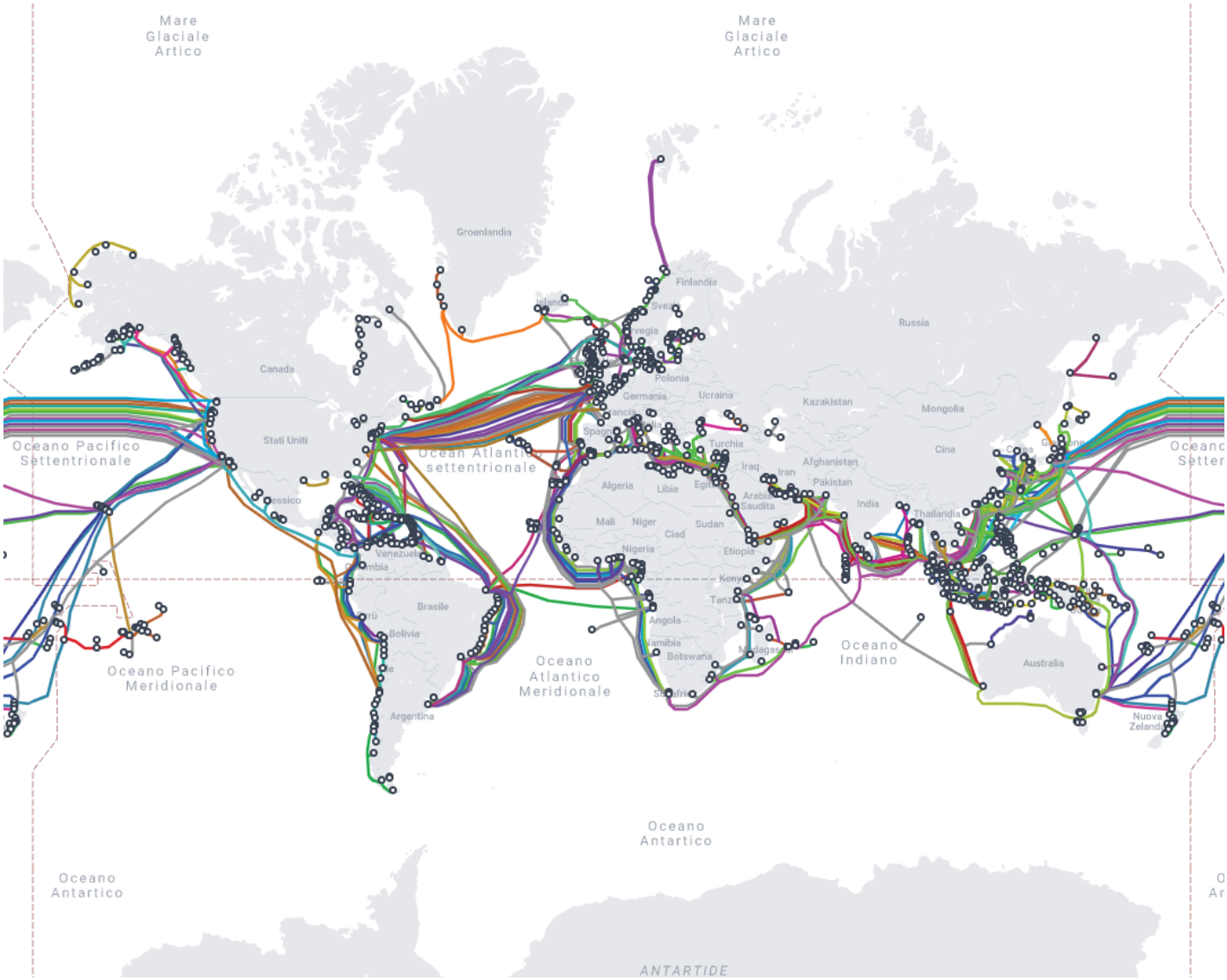


Figure 1.2 – TeleGeography's Submarine Cable Map (August 2021).

Source: https://www.submarinecablemap.com/ viewed on 23/08/2021.

Cloud providers, in effect, loan computers and networks to users round the world, from Fortune 500 companies to individuals. Providers build new services on top of their computing resources, like accessible computational linguistics, sophisticated databases, and new software development tools. Large

[10] Sposini A., Patriarca M. (2021). "La geografia del cyberspazio Cavi sottomarini, Data Center e Cloud Service Provider: tra connettivita' e competizione", *Geopolitical Brief*, n.18, pp. 1-23.

internet companies increasingly use these cloud services in lieu of building their own technology infrastructure. the expansion of cloud computing from instructional research to a billboard product generating billions of dollars in sales has commoditized computing capacity, storage, and networking bandwidth, and led to a brand-new generation of data-intensive startups. Cloud computing ties corporate decision-making driven by business risk even more closely to national security risk as one provider's supply chain decisions and internal security policies can impact several customers. This dynamic recalls the "era of huge iron," when room-sized mainframes built by some of powerful firms were how most users accessed a computer. The language of that era persists today: the vast networks of servers that cloud providers build and operate are similarly cloistered in specialized and well-protected rooms, concentrated under one or two of corporate giants. The choices these giants take about what technology to shop for, build, and operate shapes the technical environment for an increasing number of state and sensitive corporate entities. These changes in technology have had political ramifications because the growing clout of major cloud service providers causes friction between regulatory models developed for private computers and servers located in one jurisdiction and a cloud infrastructure that's globally distributed. As ever larger numbers of consumers, including intelligence and security agencies, move their data and operations into cloud services, concerns arise over where the infrastructure underneath these services is constructed and the way it's administered. Regulation of the various kinds of data within the cloud create flashpoints and misunderstanding between companies and governments. raise that a healthy skepticism from non-Western states about the dominance folks cloud providers, and also the conditions are ripe for friction.

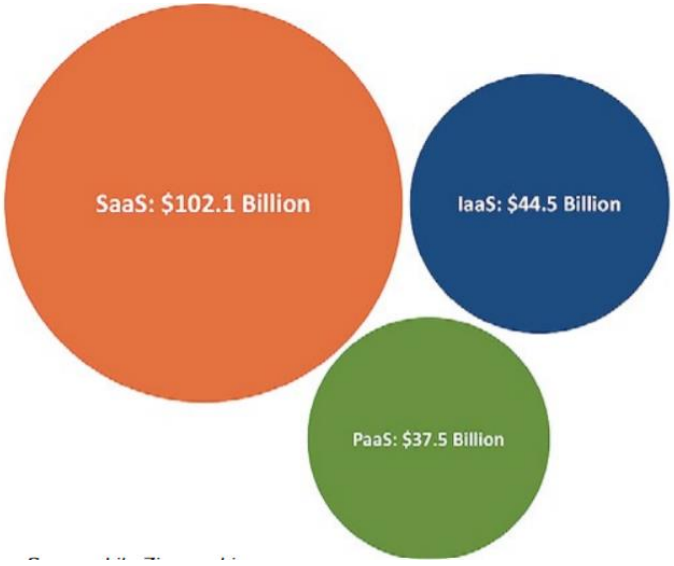


Figure 1.3 – Global Public Cloud Revenue

Source: Lily-Zimeng Liu, Herr, T. (2020). Four Myths about the Cloud: The Geopolitics of Cloud Computing.

The term cloud comes from networking diagrams where a system being described had a link to some far set of computers, a line involved to the corner of the page toward a bubbly figure representing the “other.” This bubbly cloudlike image became shorthand for computers and network services that weren't within the scope of the diagram itself but remained accessible. Caring for these ‘fleets’ of machines demands constant attention and adjustment even the simplest run processes can suffer embarrassing failures, sort of a broken Google update that caused a short-lived outage through large swaths of North America in June 2019, or a lightning strike at a Microsoft data center that hobbled Active Directory company-wide for hours. At the basis of the bulk of cloud computing is that the shared services model, where many users reside on one physical machine. Multitenancy is that the term wants to describe shared use, while the technology that produces it possible is termed a hypervisor: software that supervises a computer and divides up its resources—processor time, memory, storage, networking bandwidth, etc.—like cake at a birthday celebration where every partygoer is blindfolded. Everyone gets to enjoy their slice of cake, unaware of these around them enjoying their own portions, too. The hypervisor keeps each user separate, giving them a communicate use the pc while creating the looks that every is alone on one machine. The hypervisor is critical to keeping users isolated from each other. Flaws within the hypervisor software can enable attackers to flee from their slice of the pc into that of other users or, worse, into the host machine’s OS controlled by the cloud provider. in an exceedingly cloud service, each of those computers runs additional software selected by the cloud provider and user and every is tied into a network. By building services which use these networked machines, cloud providers can take storage at a facility in Frankfurt, match it with processing in Texas, and deliver the result to a user in Tokyo. In industry parlance, there are three basic models of cloud service:

1 Infrastructure as a Service (IaaS): These are the raw computing, storage, and networking elements that users can rent and consume sort of a service instead of a product but must largely founded and configure themselves. for instance, renting a virtual machine to host an email server.

2 Platform as a Service (PaaS): this can be the range of software and online services built on top of the cloud. Users access these services without managing the underlying infrastructure. as an example, the machine learning service an engine manufacturing company integrates into its products to predict once they will fail.

3 Software as a Service (SaaS): These are the net services that need no deep administration from the user. These services are offered without substantial ability to rewrite, rebuild, or reintegrate them like PaaS. as an example, sharing documents online or the image recognition service a hospital uses to spot tumors during a CT scan.

There are many cloud companies, most selling services in one model: some compete altogether three and therefore the largest of those are cited because the hyperscale providers— Microsoft, Google, Amazon, and Alibaba.

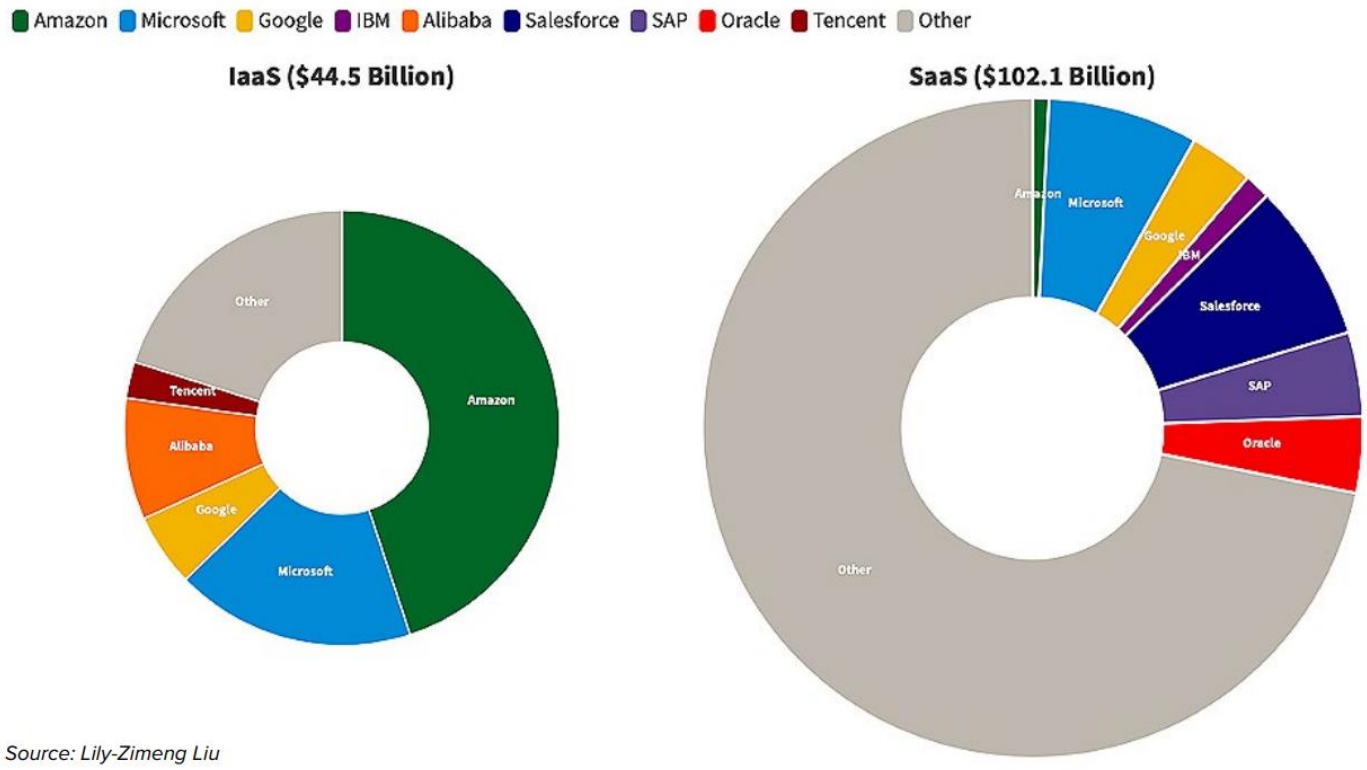


Figure 1.4 - IaaS & SaaS, 2019 Public Cloud Market Share

Source: Lily-Zimeng Liu, Herr, T. (2020). Four Myths about the Cloud: The Geopolitics of Cloud Computing.

Cloud computing is an expanding constellation of technologies—some old, some repurposed, and a few wholly new. Much of the innovation in cloud is in managing these fleets of machines and building the vast networks required to form them accessible for users, rather one snazzy new product or feature. There's nobody single model of cloud computing. the main providers all build their infrastructure in slightly alternative ways, influenced by market strategy and legacy technology investments, but the abovementioned three models help categorize what one might find within the cloud. Similarly, new is cloud providers playing host to a growing domain of conflict. There are instances where the origin and destination of an attack occurred in infrastructure owned by the identical cloud provider; attacker and defender using the identical cloud and observed (possibly interdicted) by the cloud provider. As ownership of knowledge technology (IT) infrastructure concentrates, so does exposure to what two US academics labeled the "persistent engagement" of cyberspace—with fewer and fewer major providers, there's a better likelihood of engagements that start and end within the identical network. Cloud providers need to balance the responsibilities of their global customer base with the stress of their home governments. These providers are put within the position of arbitrating between their terms of service and security commitments to customers and national intelligence and military activities happening in their infrastructure, creating a tangled web of business and national security risk. Cloud providers are geopolitical actors. Their influence reaches beyond technology markets. They influence the pace and direction of economic process, shape international security

competition, and mediate access to technologies which today inform changes within the global balance of power. The cloud is itself influenced by these same geopolitics—all of those wires and cables and boxes and bodies and their customers must live somewhere, and these jurisdictions have rules and goals all their own. The geopolitics of cloud computing demands an extended parchment than is present here, but this paper serves to spotlight, and disprove, four important myths within the relationship: 1) all data is made equal; 2) cloud computing isn't a supply chain risk; 3) only authoritarian states distort the general public cloud; and 4) cloud providers don't influence the form of the web. Technology shifts social and political dynamics. Cloud computing isn't any different, but it's quite an enormous commercial phenomenon—it influences the trajectory of states and therefore the conduct of statecraft. Conflicts in cyberspace are already being fought in and thru the cloud. As providers still concentrate unparalleled quantities of computing resources and user data, they're going to only grow in importance—as governors, as battlefields, and as magnificent engines of complexity. within the meantime, policy makers must arm themselves with quite myths as they seek to grapple with the geopolitics of the cloud.

1.3 How cyberspace affects geopolitics and international relations

In the current scenario of increasing tension at cyber level, it is essential to consider the geopolitical aspects related to this sector. Although the cyber world, as a common good open to all, also allows private actors and civil society to play a central role in the development of national and international political decisions, the centrality of state actors is still undisputed. In this perspective, the four pillars of geopolitical analysis - i.e., culture, economy, defence and politics - are elements to be considered also when analysing the reasons behind a cyber-attack. In fact, the physical aspects of cyberspace, such as servers, databases and cabling systems, are once again always present in an organised geographical area demarcated by territorial and political sovereignty. In short, geopolitics and cyberspace necessarily have elements in common, making the two disciplines closer than one might think. Although there are intrinsic differences between the two subjects in operational and ontological terms, cybersecurity and cyberspace are today central elements in international geopolitical developments[11]. The rise of the cyber domain to the 'proper' dimension of international of international relations has not been assessed by all observers with the same standards in terms of strategic relevance. According to Thomas Rid, for example, the emphasis placed on the cyber domain and cyber warfare is nothing more than a publicity stunt, because the risk of cyber war, as well as the hypothetically feared disasters, would not only never have occurred in the past and present, but certainly - Rid concludes - in the future: 'cyber war will not take place'. However, according to Joseph Nye, in the era in which we are living,

[11] Cavalieri E. (2019), Geopolitica e mondo cibernetico: incontro tra passato e futuro, dicembre, Roma: Trinità dei Monti think tank.

we are witnessing for the first time not so much a translatio imperii, (a transformation more than common in the various historical cycles), but a real diffusion of power that questions the monopoly of violence, the historical prerogative of the nation-states. This phenomenon favours the migration of power from states to non-governmental actors to such an extent that - continues Nye - "the problem with all governments in today's global information age is that there are increasing dynamics that elude even the most powerful states". In other words, interpreting Nye's analysis, one can deduce how the current cybernetic era has not only exponentially increased the information available to individuals, who can communicate by bypassing bureaucratic censorship and national borders, but has also fostered an increasing role of non-state actors. Furthermore, Nye's analysis shows how the technological revolution has favoured the distortion of the very concept of 'power' in the dynamics of international politics, dragging the system towards a process of s-politicisation of violence. In fact, the increase in the diffusion of ICT technologies in the field of warfare, as well as the relative absence of a threshold of access to such instruments, have caused the classic concept of weapons to be surpassed, since apparently peaceful objects, designed and produced for civilian use, have been transformed into offensive means of global scope. In the information age, the distinction between military and civilian has disappeared, not so much in terms of the division of roles, but rather in terms of overturning the modern concept of the battlefield. It is certainly not petty alarmism to reach the awareness that the modern means made available by today's technological discoveries, combined with the now definitive achievement of the globalisation 'of services and people', are able to make everyday life a real theatre of war, in which each one of us can be considered not only a target, but also a potential indirect perpetrator of a hostile act[12].

The increasing societal dependence on information and communication technologies (ICTs) in the least levels has changed the way during which individuals interact nowadays, both personally and professionally. But has it done the identical for states? Have the standard power loci been plagued by the event of latest technologies to such an extent that their routine and their theoretization be challenged? The role of technology in society has long been acknowledged by highly influential thinkers, like Marx, Max Weber or sociologist, yet it's remained marginal to their work, being essentially limited to serving economic ends. By mid-twentieth century, the Frankfurt School placed a central emphasis on the employment of technology for the subjugation of the masses by the fashionable state and opened the door for critical theories that account for the ICT-driven transformation. The latter has been addressed in numerous ongoing discussions associated with power-embedded entities, however, these conceptualizations lag behind. The cyberspace has triggered a series of economic, social and political adjustments from the local to the international arenas. Moreover, security has been brought back to the forefront united of the most important concerns affecting the way during which states interact. ICTs have impacted the relations involving international organizations, their constituencies, and other

[12] Martino, L. (2018). La quinta dimensione della conflittualità. L'ascesa del cyberspazio ei suoi effetti sulla politica internazionale. *Politica & Società*, *7*(1), 61-76.

stakeholders of the data society, by fostering the event of horizontal networks, which have supplemented, instead of replaced, the prevailing hierarchies. Presently, the international institutional architecture for the governance of the cyberspace is dominated by a multiplicity of initiatives geared toward increasing cooperation at the international level, likewise as by a redefinition of the roles played by existent actors. Such dynamics is observed within the discourse over security within the cyberspace, as a milestone for the expansion of the knowledge society. So far, states have strongly pushed for empowering existent global institutions to require up new cyber responsibilities and to reshape their agenda accordingly. Attempts at developing negotiation (IR) theories relevant for the knowledge society have remained rather scarce, primarily because of the inner-looking focus of the discipline. Different endeavors at framing conceptual frameworks have rarely built on one another for advancing a comprehensive conceptualization or for developing middle-range theories supported interdisciplinary approaches. Currently, at the international level, a minimum of 19 global and regional organizations are actively involved within the security and governance of the cyberspace (Government Accountability Office 2010). This growing number reflects a standard understanding that the challenges posed by the spread of ICTs can't be tackled by states in isolation; yet, up to this, such international engagement was primarily directed towards limitation and cooperation within the cyberspace. The unique governance challenges led to by the expansion of the web have also given rise to emerging transnational institutions, like the web Corporation for Assigned Names and Numbers (ICANN) or the net Governance Forum. At the national level, more and more states retask existing institutions or establish new ones to oversee the flow of data in computer-mediated environments. While states still exert authority and control over both physical infrastructure and over the net content, more and more non-state actors challenge their position. The cyberspace has become a replacement domain of power, that the monopoly is not any longer exclusively held by governments[13]. In jurisprudence circles, researchers agree that a "legal regime likeminded to the actual characteristics of cyber-attacks" is important, but problematic to define. Despite the US government's "International Strategy for Cyberspace", the legal rules are ambiguous, and complicate military thinking. Lawyers within the govt have raised such a big amount of crippling legal questions on cyber warfare that they need left our military unable to fight, or perhaps plan for, war in cyberspace. Some argue that the Law of Armed Conflict sets minimum standards, but the Law of Armed Conflict was designed to resolve conflicts fought primarily with kinetic weapons, to not resolve a cyber conflict. It is difficult to attribute state responsibility for cyber-attacks, as they're difficult to trace, and governments may hire "hackers" to try and do the task for them. the character of cyber-attacks makes it possible to hide their true origin. This has led some to conclude that it's not criminals but states that pose the best threat to global cyber security within the international system: it's difficult to divide the threats to Internet

[13] Radu, R. (2014). Power technology and powerful technologies: global governmentality and security in the cyberspace. In *Cyberspace and International Relations* (pp. 3-20). Springer, Berlin, Heidelberg.

security between these two groups, even as the link between organised crime and also the state is increasingly blurred. In mediation and social science, the discussion focused on how cyber weapons are part of state power. Technical circles have emphasised the complexity of the enormous global 'cyberspace', and stressed the character of this phenomenon, which easily and sustainably transcends any national borders. At present, the international situation about cyber weapons is like that of nuclear weapons before the Non-Proliferation Treaty. Several cyber superpowers (the us, China, Russia, and Israel) have developed and deployed cyber weapons either defensively or offensively and have used them albeit not extensively. Countries are struggling to make their cyber capabilities behind the nice Wall of Secrecy characteristic of the national security state. Similarly, like the event of nuclear weapons, fear and uncertainty about the results of cyber warfare act as powerful forces driving this virtual race. However, the doubtless devastating effects of cyber warfare are serious enough to form it possible to realize a consensus on controlling the proliferation of those weapons. Even if the scope of the international convention is proscribed to government-on-government attacks, the international community remains faced with the daunting problem of rapidly evolving technology. The theoretical complexity of the technological dimension isn't well understood, as there are an almost incalculable number of interrelated networks and systems. For other international treaties, like the Kyoto Protocol, the pace of technological change is measured in decades, which supplies sufficient time to figure out the main points of a convention. However, within the cyber sphere, the pace of technological change is measured in weeks or at the best months, making it difficult to draft precise definitions and protections against cyber-attacks[14]. Despite the importance of the matter posed and therefore the great qualities of the Roche & Blaine proposal on the adoption of a world Convention for the peaceful use of cyberspace, the political, legislative and technical difficulties of effective control with a view to Internet security are very real. Regarding the political difficulties, states, especially the foremost powerful ones, can be reluctant to sign such a convention. Why cooperate on cyber issues when it's the balance of power that prevails in international relations? While their sovereignty is factual contested and obstructed, is it no more pertinent for them to entrust the management of those new problems to their own structure? What confidence are often placed within the supposedly positive effects of a global convention during this area? Wouldn't or not it's better to form real strategic IT superiority effective internally? Another difficulty is that this phenomenon ignores traditional geographical frontiers (land, air, sea). How can we organise international cooperation between governments under these conditions, when it involves 'combating a phenomenon that builds its power and spreads outside any traditional geographical concept of your time and space'? How can we also organise better global governance and Internet security when 'most user countries aren't democracies and it's therefore difficult to think about giving them power over the architecture and regulation of the Net'?

[14] Roche, E. M., & Blaine, M. J. (2013). Convention internationale sur l'utilisation pacifique du cyberespace. *Netcom. Réseaux, communication et territoires*, (27-3/4), 309-330.

The legal difficulties are thanks to the restrictions on freedom of exchange and therefore the greater capacity for intrusion or surveillance by regulators: 'there isn't any common legal basis between States on which to harmonise practices'. In addition, one mustn't ignore the technical difficulties of any adequate response by the State that's the victim of a cyber-attack. whether or not a cyber-attack on the networks, servers or software of 1 state is proven, how can it's have interpreted as actually resulting from an attack caused by another state? the benefit of access to digital technologies by non-state hackers (mafias, terrorist organisations, private individuals) makes the interpretation non-obvious and also the possible cyber response perhaps irrelevant[15].

1.4 Use of cyberspace by Islamic terrorism

The term cyber-terrorism was first mentioned within the 1980s by Barry Collin. Collin claims that the convergence of those two worlds, virtual and physical, is that the explanation for cyber-terrorism. The convergence in question is cyberspace and terrorism. Cyberspace is an abstract domain and describes the virtual world where computers and networks operate, while the physical world is that the place where we live. The convergence that develops from the physical and virtual world becomes more complex and offers rise to cyber-terrorism. Cyber-terrorism or terrorism in cyberspace has been defined because the use of computers and therefore the internet in terrorist activities. within the other hand, cyberterrorism indeed uses computers and also the internet for his or her activities that violate the law and to intimidate the govt accordingly to attain their goals. during this case, terrorists and therefore the internet are closely interrelated. the net has become a forum for terrorist groups and individual terrorists to spread messages of hatred and violence. Terrorists use encrypted email to plan the actions of websites of terrorist groups that reach political and social agendas. Cyber-terrorism could be a cybercrime qualified in transnational crimes because it consists of crimes committed by terrorists' cross-national borders. Conceptually, transnational crime may be a crime that crosses the state. this idea was first introduced internationally within the era of the 1990s at an international organisation (UN) meeting which discussed matters regarding crime prevention. On November 15, 2000 at the 62nd plenary meeting in Palermo, Italy, the global organization adopted a convention against all sorts of organised transnational crime or better called the world organisation Convention Against Transnational gangdom (UNCATOC)[16]. The potential threats of attacks by terrorists in cyberspace would concentrate on systems and networks that contains critical information infrastructure. it should include conducts against the confidentiality, integrity and availability of such systems

[15] Bakis, H. (2013). Fragilité du géocyberespace à l'heure des conflits cybernétiques. *Netcom. Réseaux, communication et territoires*, (27-3/4), 293-308.

[16] Kadir, N. K., Judhariksawan, J., & Maskun, M. (2019). Terrorism and cyberspace: A phenomenon of cyber-terrorism as transnational crimes. *FIAT JUSTISIA: Jurnal Ilmu Hukum*, *13*(4), 333-344.

and networks through cybercrimes: illegal access, illegal interception, data interference, system interference, and misuse of devices. Serious hindering of the functioning of a computer systems and networks of the critical information infrastructure of a State or government would be the foremost likely targets. The dependency of data and communication technology creates at the identical time a vulnerability that's a challenge for cyber security. Attacks against critical information infrastructures may cause comprehensive disturbance and represent a major threat which will have the foremost serious consequences to the society. Potential targets are also governmental systems and networks, telecommunications networks, navigation systems for shipping and traffic, water control systems, energy systems, and financial systems, or other functions of significant importance to the society. It should constitute a criminal offence when terrorists are able of hindering or interrupting the correct functioning, or influence the activity of the pc system, or making the system inoperative e.g., crashing the system. Computer systems can thus be closed down for a brief or extended period of your time, or the system may process computer data at a slower speed, or run out of memory, or process incorrectly, or to omit correct processing. It doesn't matter if the hindering being temporarily or permanent, or partial or total[17]. Contemporary Islamist terrorism is communication, and also the e-jihad represents its progressive evolution towards the cyberspace. The use of Internet by the promoters of jihad has generated a radical change in Islamic fundamentalism, introducing new problems which have have intensified the complexity of the phenomenon. The Internet was born from the interweaving of a multiplicity of networks of a heterogeneous nature and its highly decentralized architecture guarantees an unprecedented speed of renewal. Hyper-terrorism is today an organism that's constantly evolving in its appearance, characters and process, and exhibits a nature which isn't any longer so obvious or probable. The cybernetic manifestation of the battle of the mujahideen is realized within the possibility of developing innovative measures and within the diffusion of extremely heterogeneous material for the formation of the militant and for the diffusion of the ideology of the movement. In a particular way, within the strategy of the Islamic fundamentalists, the online assumes a double valence in the strategy of the Islamic fundamentalists: acting within the group, it acts as a channel of re-satiation, favouring the sense of aggregation of the members and therefore the sharing of resources; externally, it's a legitimate instrument of promotion of the Jihadist cause. The online jihadist infrastructure consists of a multiplicity of internet sites that disseminate material in an exceedingly capillary manner. Specifically, analysts of the phenomenon distinguish between distributor sites, producer sites and key nodes, consistent with the prevailing function they play within this digital architecture. The peculiar aspect of the jihadist sites is that they operate through significant interactions in what's a real network of resource sharing. The potential of those pages also manifests itself in their extreme elusiveness, whereas if a terrorist website is taken down, it'll soon reappear under another name and/or on the server of another service provider. The videos of propaganda and executions emerge as a privileged component for the promotion of the

[17] Schjolberg, S. (2007). Terrorism in Cyberspace-Myth or reality.

movement and also the propagation of fear. Specifically, it's possible to watch a good evolution within the conception and editing of the films: in an exceedingly few years the militants have gone from scenographies that noted divine revelations in natural caves to videos made with more sophisticated techniques, like the one released in September 2014 entitled Flames of War. The documentary, lasting about 55 minutes and simply available online, features a montage with cinematic content and various camera work that add explosions to the pictures. To support the training of these who cannot physically attend the training camps, actual terror manuals distributed online are created, which offer the aspiring jihadist with ideological bases and operational instructions. Inspire and Dabiq are currently the foremost renowned magazines of the Islamic State and are considered, respectively, the official voices of al-Qaeda and Isis. Fundraising is solicited by jihadists through chats, emails, forums, often hiding behind charities or elaborating real scams through the manipulation of non-public data. As counter-terrorism expert Charles Shoebridge puts it, "the government has realized that several refugee relief organizations, humanitarian and charitable organizations are literally acting as a canopy to lift funding for terrorist organizations." The recipients of the jihadist message on the web are supporters, sympathizers, mujahideen, potential recruits, popular opinion. and so there's the enemy. In addition to the necessity to succeed in and train new potential recruits, the objectives of online jihadist terrorism are mainly geared to discredit the enemy and frighten the general public, performing on different levels. The first mechanism used is that of demonization, which is closely connected to the advantageous confrontation: the militants describe their behavior as a necessary sacrifice, well-liked by Allah, because it responds to the cruelties that the West - devil has inflicted on their people. The strategy of dehumanization operates during a similar way which, through the attribution of despicable qualities, creates a psychological distance between the perpetrator and also the victim, alleviating the sense of guilt and stimulating violent action. Delegitimization, allotted through the attribution of blame and also the distortion of certain events, has the clear objective of constructing the enemy lose prestige and credibility within the eyes of citizens and potential new members. The vulnerability of adversaries is of significant importance to confirm the success of operations associated with the consolidation of the Umma ideal. The language is employed instrumentally to favor the creation of a fundamentalist group identity, activating dynamics of total closure towards what moves removed from its own cultural references. Although little is thought about the cyberspace offensives meted out by ISIS, several indicators suggest that the organization has made important progress during this area. Primarily, the Islamic State is headed by a gaggle of young leaders who have considerable skills and knowledge within the cyber sector - also accumulated due to the past stock within the ranks of al-Qaeda - and with considerable knowledge of latest technologies. In the Dark Web of the forums, ISIS sympathizers share photos and videos of the cockpits of varied aircraft discussing the way to virtually enter the on-board controls to crash passengers, still as bypass the security systems of nuclear plants to cause release. of radioactive substances. Twitter accounts people magazines and personal TVs have often been hacked via "deface" - modification of

the pages and also their contents - through the image of a person with a covered face and the adjacent phrase i like you ISIS. Pragmatically, however, the successes of the Islamic State in cyberspace have thus far been limited, despite the very fact that the US has sued Ardit Ferizi, a Kosovar who entered the U.S. last October. security data and stole personal information (emails, passwords, locations and phone numbers) of over 1,350 military and personnel governmental. Ferdizi later sent the information to Junaid Hussain, a member of the Islamic State Hacking Division (ISHD) who was killed in an August raid in Syria and located guilty of publishing British Prime Minister Blair's private addresses and telephone numbers in 2012. additionally, he used Twitter under the pseudonym of Abu Hussain al-Britani, calling for violent attacks on Israeli diplomats and inspiring new recruits to visit join ISIS. Analyzes published in September 2014 by the US intelligence company Intel Crawler indicate a dramatic increase within the use of the virus (njRAT) in 4 main Iraqi cities - Baghdad, Basra, Erbil and Mosul - linked to ISIS. In conclusion, while within the field of social networks and propaganda it's achieved great successes - which have provided it with foreign fighters, funds and advertising - up to now the Islamic State has did not conduct any operation in cyberspace capable of substantially threatening Homeland Security of any country, nor are there any factors that indicate it'll reach the short-term period. Despite this, on bissextile day, the US declared that it had conducted cyberwar operations against ISIS, the primary time in Washington's history that such attacks during an ongoing war. The main objective is to isolate Isis both physically and virtually, limiting its ability to conduct operations by disturbing its communication systems (while keeping them active for any position detection) and also the introduction of malware or viruses[18]. The Islamic State has taken cyber-enabled strategies and tactics farther than any previous political movement, which is why its behaviour in cyberspace has become a counter-terrorism crisis. This crisis suggests that policy and law, including law, crafted before the Islamic State became a threat, did not prevent the group from making cyberspace a strategic asset. This failure prompts the necessity for brand new approaches, but, at present, more disagreement than consensus exists among states- and even within states- on a way to deal with the crisis. In law of nations, the Islamic State's cyber-enabled activities have least battered the foundations on suppression of terrorist financing. Under treaty law and binding SC mandates, states have obligations to prevent the financing of terrorism. However, the Islamic State's finances rely totally on funds generated within territories it controls, like taxes, oil revenues and criminal schemes (eg ransom kidnapping, selling looted antiquities). Although the system to suppress terrorist financing limits the Islamic State's ability to maneuver large sums through formal channels, the Islamic State

[18] Lay S., Pascarella M. (2016), "L'utilizzo del cyberspazio da parte del terrorismo islamico", *Alpha Cyber Security Research Projec*t, marzo, Roma: The Alpha Institute of Geopolitics and Intelligence.

has managed to fund itself. The system isn't necessarily broken, but it's limitations when terrorists have funding not liable to foreign and global financial mechanisms[19].

1.5 The desire for sovereignty: independence in cyberspace

The geographical element plays a fundamental role in geopolitical analysis: the physical appearance of a territory, its position on the world, its distance from other territories or sources of resources, etc., are all aspects to be considered within the spatial analysis, however, it's necessary to think about a series of other factors without which the analysis would be disconnected from reality, namely cultural, demographic, religious and political of a given territory. The first difficulty is encountered at the very beginning of the work, when it involves determining whether it's possible to think about cyberspace as a territory to which the above factors is applied. On now, however, we are able to consult with some studies that theorise the understanding of cyberspace as a geographical space by comparing the empirical attributes of a territory - as defined by Jean Gottmann - with the characteristics of cyberspace: it's continuous, but limited, expanding, but diverse, it's compartmentalised and organised. Cyberspace has its own human geography, which is becoming increasingly relevant in geopolitical analyses, the more relevant the sorts of sociality in cyberspace become. From the top of the 1980s to today, because of an extended series of technological and cultural phenomena generated within the u. s., the worldwide cyber-arena has been subject to American domination from the purpose of view of technological superiority and controls regarding security and certifications, the globe Wide Web itself was born internally within the u. s.. additionally, because the network of networks increases its nodes and its connections becoming more and more pervasive, the necessity for its regulation is felt more strongly. And it's precisely within the USA that the requirement for global governance of the network is most felt. within the time period of the net, the management of registry functions associated with Internet Protocol (IP) addresses were handled by the Defense Advenced Research Projects Agency (DARPA), bureau employed by the Pentagon, and by the University of South Carolina. In 1998, ICANN (Internet Corporation for Assigned Names and Numbers), which however is subject to stringent stipulations and strict supervision by the us government. To date, there are 1,292 top-level domains (TLDs), compared to the first seven from the 1980s. In fact, in 2012, ICANN liberalized generic Top-Level Domains (gTLDs), initiating a robust expansion of registrations and assignment requests. Today cyberspace is an integral a part of contemporary society, within it the lives of citizens and also the actions of states happen in parallel and at the identical time we try and define policies for the subjugation of cyberspace to state authority. Although today we are removed from a world governance of the cyber space, different interests and demands find yourself entering this process. The

[19] Fidler, D. P. (2016). Cyberspace, terrorism and international law. *Journal of Conflict and Security Law*, *21*(3), 475-493.

first claim during this sense is that the famous "Cyberspace Declaration of Independence", written in 1996 by John Perry Barlow which states in its first lines "Governments of the economic world, you tired giants of flesh and steel, I come from Cyberspace, the new place of the Mind. within the interest of the longer term, I ask you, who are a part of the past, to go away us alone. you're not welcome among us. you've got no sovereignty within the place where we meet. ». But if Barlow's declaration was addressed to any or all governments of the "industrial world" and proclaimed the independence of the whole cyberspace from the physical world, today new independenceist declarations concern physical territories, communities that don't see their claims recognized by the " tired giants" and seeking freedom in cyberspace. A recent example is that the case of geographical area, which in 2014 obtained the. krd domain from ICANN to be assigned to the sites of the geographical area Regional Government, to institutions, to universities and to those that (in Kurdish language) will promote their belonging to the Kurdish community. Although ICANN attributes two-letter domains (ccTLDs) to states, Hiwa Afandi, the pinnacle of the Kurdish government's Information Technology Department, which managed the popularity process, commented on the event: imprisoned in these geographic boundaries don't have the identical influence in cyberspace. On the net we've chosen our borders", adding that ".KRD may be a national symbol; it's our flag in cyberspace ». But the case that constituted the precedent to cyberindependence dates to 2005, with the assignment to Catalonia, after a battle with the central government (which had denied the two-character. ct domain, reserved for nation-states), of the domain. cat, which "legitimized the existence of a cultural community on the web". the selection to deploy independence aspirations in cyberspace therefore arises from the requirement for recognition of linguistic and cultural autonomy by a community that feels constrained within the state context during which it's located. Another community tenaciously linked to its autonomy and in perennial struggle for independence from central power is Scotland, which on 15 July 2014 officially adopted the .scot domain for Scottish language and culture sites31 and on 17 February 2015 the Scottish Government relocated government websites and initiated infrastructure changes and also the relocation of staff email addresses. The domain is managed by DotScot Registry, a non-profit organization established in September 2009 specifically to request and manage the. scot domain. While outside of Scotland having a .scot domain could seem of little relevance, for Scottish separatists it's a crucial thanks to express their autonomy, to align themselves as Scots and not British, to precise what most of the Scots see it because the fundamental identity. In this short study we've got tried to supply a very partial overview of the new phenomenon of cyber independence, and more generally of the displacement of political movements and actions and of demands from their traditional terrain of struggle in cyberspace. Today, as we've seen, there are several communities that demand independence or a minimum of autonomy from a central power that they recognize as 'too many', which within

the wake of the Catalan example are turning to cyberspace to say their requests, meaning it united space still free from state intrusiveness[20].

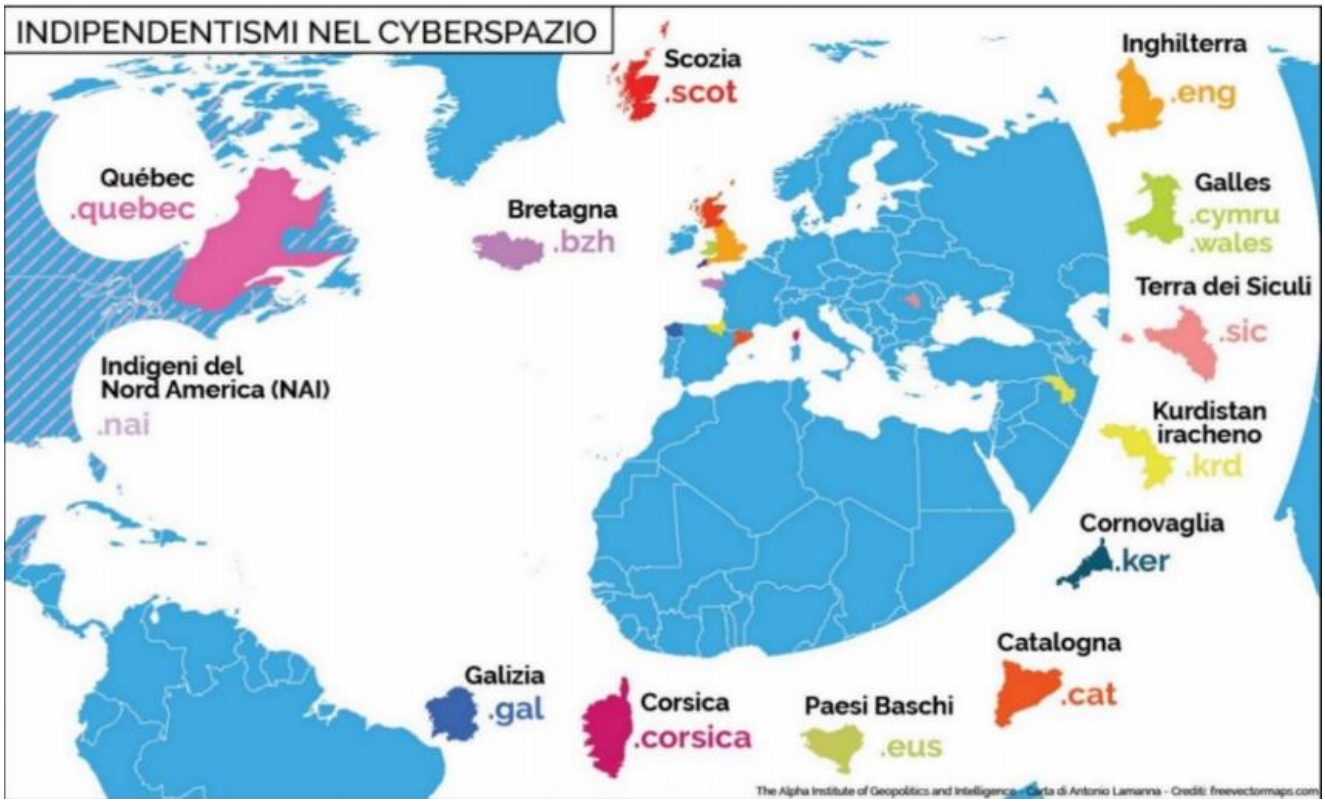


Figure 1.5 – Independence in cyberspace

Source: Lamanna A. (2016), "Revival etnico 2.0. Indipendentismi nel cyberspazio", *Alpha Cyber Security Research Project*, settembre, Roma: The Alpha Institute of Geopolitics and Intelligence.

[20] Lamanna A. (2016), "Revival etnico 2.0. Indipendentismi nel cyberspazio", *Alpha Cyber Security Research Project*, settembre, Roma: The Alpha Institute of Geopolitics and Intelligence.

Chapter 2

The instrument of sanctions

2.1 UN legislation and its sanctions system

To analyse the instrument of sanctions in their entirety, it's of primary importance to initiate a study that takes account of varied factors and, at the identical time, can provide answers to the various doubts and questions that arise to the present institute. Contemporary law contains various ways and means (apart from diplomatic means and recourse to institutional instruments) through which to react to the committing of a bootleg act, i.e. the violation of a world obligation. the most ones are (i) the regime of international responsibility of States and international organisations for wrongful acts, and (ii) the regime of sanctions. Of obvious interest during this work is that the second type: the sanctions regime. As is well-known, this operates outside general jurisprudence and isn't merely a consequence of the wrongful act. Sanctions have several dimensions. In contemporary law, the peculiarity of sanctions within the technical sense lies in their institutionalisation: they're therefore collective measures decided or recommended by international organisations[21]. In this regard, it had been certainly the international organization Charter that took the crucial step. Chapter Seven of the Charter created an institutionalised system for imposing collective sanctions on states deemed liable for threats to the peace, breaches of the peace or acts of aggression. After all, world organisation was created immediately after the Second warfare and therefore the primary mandate is peacekeeping. For this reason, the articles contained in Chapter Seven of the Charter represent powers which will be employed by the protection Council to confirm the most goal of the international organisation[22]. The fundamental difference between the meaning of sanctions within the national context and also the popular understanding of sanctions within the international context is that the action commonly noted as sanctions within the international sphere doesn't necessarily serve the aim of enforcing a legal norm. this may even be the case with UN sanctions, because it isn't a requirement that they be applied in response to a violation of Charter obligations. Thus, they will be interpreted as 'political measures' which the protection Council has the 'discretion' to use to keep up or restore international peace and security[23]. This is

[21] Silingardi S. (2020), *Le sanzioni unilaterali e le sanzioni con applicazione extraterritoriale nel diritto internazionale*. Milano: Giuffrè Francis Lefebvre.

[22] Gordon R. J. F., Smyth M., Cornell T., (ed.), (2019), *Sanctions law*. Oxford, UK; Portland, Oregon: Hart Publishing.

[23] Farrall J. M. (2007), *United Nations sanctions and the rule of law*. New York: Cambridge University Press.

made perfectly clear in Article 39 and, subsequently, Article 103 provides an additional indication of the supremacy of the UN Charter.

Indeed, where a Member State includes a conflict between the Charter and the other international agreement, the provisions of the UN Charter will prevail.

Box 2.1 UN Charter – Article 39 and Article 103
Chapter VII – Article 39

The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.

Chapter XVI – Article 103

In the event of a conflict between the obligations of the Members of the United Nations under the present Charter and their obligations under any other international agreement, their obligations under the present Charter shall prevail.

It is also well-known that the Charter determines - in Articles 40, 41 and 42 - a series of measures that political scientists and commentators have over time defined because the principle of gradualness. Initially, provisional measures are proposed to avoid a worsening of the situation; later, measures not involving the employment of force – e.g., total or partial interruption of diplomatic and/or economic relations –; Eventually, if the previous measures are judged inadequate or have proved inadequate, any action aimed toward restoring peace may be taken, including actions involving the employment of force. Without a doubt, the primary years after the birth of the United Nations were the foremost complicated. The tip of the Second World War had brought with it several unresolved territorial disputes and it had been up to the newly created world organization to point out the most effective thanks to settle the assorted disputes currenti, in particular to demonstrate to the entire world – member states and non-members – its capacity and credibility in pursuing the three objectives announced in Article 1 of the Charter. By way of example, one in all the primary tests was certainly the withdrawal of Anglo-Soviet armies from Iran. These and lots of other national and international challenges to peace and security were dropped at the eye of the Council. None, however, could overpower the East-West hegemonic interests that now possessed all international security questions. As quickly because the British and other European colonial powers dismantled their overseas dominion, the newly independent states were engulfed within the East–West standoff. There was no lack of bloody conflicts with the wars between Pakistan, East-Pakistan and India, the Israel–Palestine conflict, the Greek–Turkish fight over the control of Cyprus, the struggle of Indonesia to forbid the old Dutch colonialists from retaking power,

confrontation between the Koreas, the Berlin Blockade, and therefore the high-noon of the conflict, when the US and therefore the Soviets faced off with drawn guns over the Cuban Missile Crisis. the understanding of a veto deterred any request for council intervention. With the safety Council paralyzed by superpower politics, those that favored the creation of the UN for its lofty promises, now recognized that, like its predecessor the League of states, it seemed doomed to fail. After only three years, Trygve Lie, the primary administrator, saw himself forced to publicly declare "the UN isn't expendable". He further set straight, during a New York Times article, many misperceptions about the UN's performance and defined the finer technical points of application of the veto under Chapter VII of the UN Charter[24].

Box 2.2 Trygve Lie Appraises the Future of the U.N.—New York Times 9 May 1948

A permanent member that is party to a dispute must abstain from voting when the Council is acting for the pacific settlement of that dispute. Actually the practice of voluntary abstention has been growing in the Security Council even when the permanent member is not a party to the dispute… Only when acting under Chapter VII of the Charter, when the use of sanctions or force is likely to be involved, do the permanent members possess a full power of "veto". Even here the power of "veto" is not unlimited. If a permanent member or one of its allies should ever commit an act of armed aggression, the Charter provides a means whereby any "veto" it might exercise in such circumstances would be worthless. Article 51 of the Charter expressly reserves to the member nations the right of collective self-defense "if an armed attack occurs against a member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security."

The Secretary General's initiative didn't change the stalemate within the SC markedly. in a very 1950 analysis of the UN's legal footings and their practical applications, Swedish jurist Alf Ross commented: "The SC has become a battlefield of the policies of the nice powers, and therefore the veto right has been used as a weapon during this struggle" (Ross 1950). The extraordinary and extremely obvious overuse of the veto power by Russia was a awfully visible symbol for the deeply divided post-war world vision: 80 Russian vetoes within the first nine years of the protection Council's existence against a complete of 5 for all other P5 member states raised the question of whether the Council would ever be during a position to measure up to its mandate[25].

[24] Lie T. (1948), "Trygve Lie Appraises the Future of the U.N.", *New York Times*, May 9, p. 175, 182, 184.

[25] Carisch E., Rickard-Martin L., Meister, S. R. (2017), *The Evolution of UN Sanctions From a Tool of Warfare to a Tool of Peace, Security and Human Rights*. Springer International Publishing AG.

Table 2.1 – Use of veto by permanent five member states

Period	China	France	Britain	US	USSR/Russia	Total
Total	18	18	32	86	146	300
2020	2	-	-	1	2	5
2019	3	-	-	-	3	6
2018	-	-	-	1	2	3
2017	1	-	-	1	5	7
2016	1	-	-	-	2	3
2015	-	-	-	-	2	2
2014	1	-	-	-	2	3
2013	-	-	-	-	-	-
2012	2	-	-	-	2	4
2011	1	-	-	1	1	3
2010	-	-	-	-	-	-
2009	-	-	-	-	1	1
2008	1	-	-	-	1	2
2007	1	-	-	-	1	2
2006	-	-	-	2	-	2
2005	-	-	-	-	-	-
2004	-	-	-	2	1	3
2003	-	-	-	2	-	2
2002	-	-	-	2	-	2
2001	-	-	-	2	-	2
2000	-	-	-	-	-	-
1999	1	-	-	-	-	1
1998	-	-	-	-	-	-
1997	1	-	-	2	-	3
1996	-	-	-	-	-	-
1986- 1995	-	3	8	24	2	37
1976- 1985	-	9	11	34	6	60
1966- 1975	2	2	2	12	7	33
1956- 1965	-	2	10	-	26	31
1946- 1955	(1[b])	2	3	-	80	85

Table of own production; Data compiled by Global Policy Forum with Information from the United Nations.

Website:https://www.globalpolicy.org/component/content/article/102/32810.html (last access on 19 July 2021) [b] The data reflects vetoes by the Republic of China (Taiwan) who held the Chinese seat on the Security Council from 1946 to 1971. It used the veto only once, to block Mongolia's application for membership in 1955. The first veto exercised by the People's Republic of China was therefore not until 25 August 1972

The United Nations in the 1950s had to deal with a series of crises in the Middle East and Asia (two Koreas) and because of Mao Tse Tung's Chinese revolution. The Soviet Union wanted China's seat at the UN to be given to Mao, but for a long time, China was represented by a government that exercised control over a minimal territorial portion. The issue would only be resolved in 1972. However, in 1950, the Soviet Union decided to boycott Security Council meetings by not turning up. Decisions must be taken with the presence of all member states of the Council. The US circumvented this rule and decided to intervene in support of South Korea with a US-led coalition of states under the auspices of the UN. However, a change to Article 27, whereby deliberations can be taken even in the absence of one of the permanent members, has not been established in practice. In 1950, it was the General Assembly that adopted a resolution that was very important at the time: Resolution 377/1950, called 'Uniting for Peace'. The latter extended powers in the field of international peacekeeping and security. The resolution was adopted when the Security Council was blocked by cross vetoes. It was, therefore, necessary to provide for the possibility of UN intervention outside the Security Council. The idea of the Uniting for Peace resolution is that the General Assembly intervenes and takes over with a recommendation from the Council which is blocked by the vetoes of the permanent members. If the restricted body, due to the lack of unanimity among the permanent members, fails in the exercise of its primary responsibility of maintenance of international peace and security, and if the requirements of Article 39 are met, the resolution allows the General Assembly to consider the situation immediately to adopt appropriate recommendations for the adoption of collective measures, which may also include the use of armed force, to maintain or restore international peace and security.

If the Assembly is not in session, a special session, called the Emergency Special Session, is convened. This is an ad hoc session, convened based on Resolution 377 of 1950 so that the situation can be debited within 24 hours and the necessary recommendations adopted.

Thus, with Resolution 377, the General Assembly can act as a full replacement for the Security Council. Uniting for peace will essentially be applied in two contexts:

1. To create an actual peacekeeping mission that the General Assembly has created. The first and only mission created, based on resolution 377, is the 1956 UNEF I (United Nations Emergency Force I) mission that stepped in during the Suez crisis.

2. To convene special emergency sessions of the General Assembly, among the main ones:

Middle East '56

Hungary '56

Middle East '58

Congo '60

Afghanistan '80

Occupied Arab Territories

These are typically international crises where vetoes by the permanent members prevented the Security Security Council from taking appropriate peacekeeping measures. Lastly, it is relevant to specify the Security Council structure: in fact, the UN restricted body establishes sanctions committees, composed of all Council members, which are tasked with implementation of sanctions regimes. These committees are most often chaired by non-permanent members of the Council. The Council also often establishes expert groups (frequently called Panels of Experts) which support the work of committees. Most members of these groups are based in their home location, while two are based in New York and one in Nairobi. In addition to providing secretariat support to committees, the Security Council Affairs Division (SCAD is responsible for recruiting, managing and supporting these expert groups.

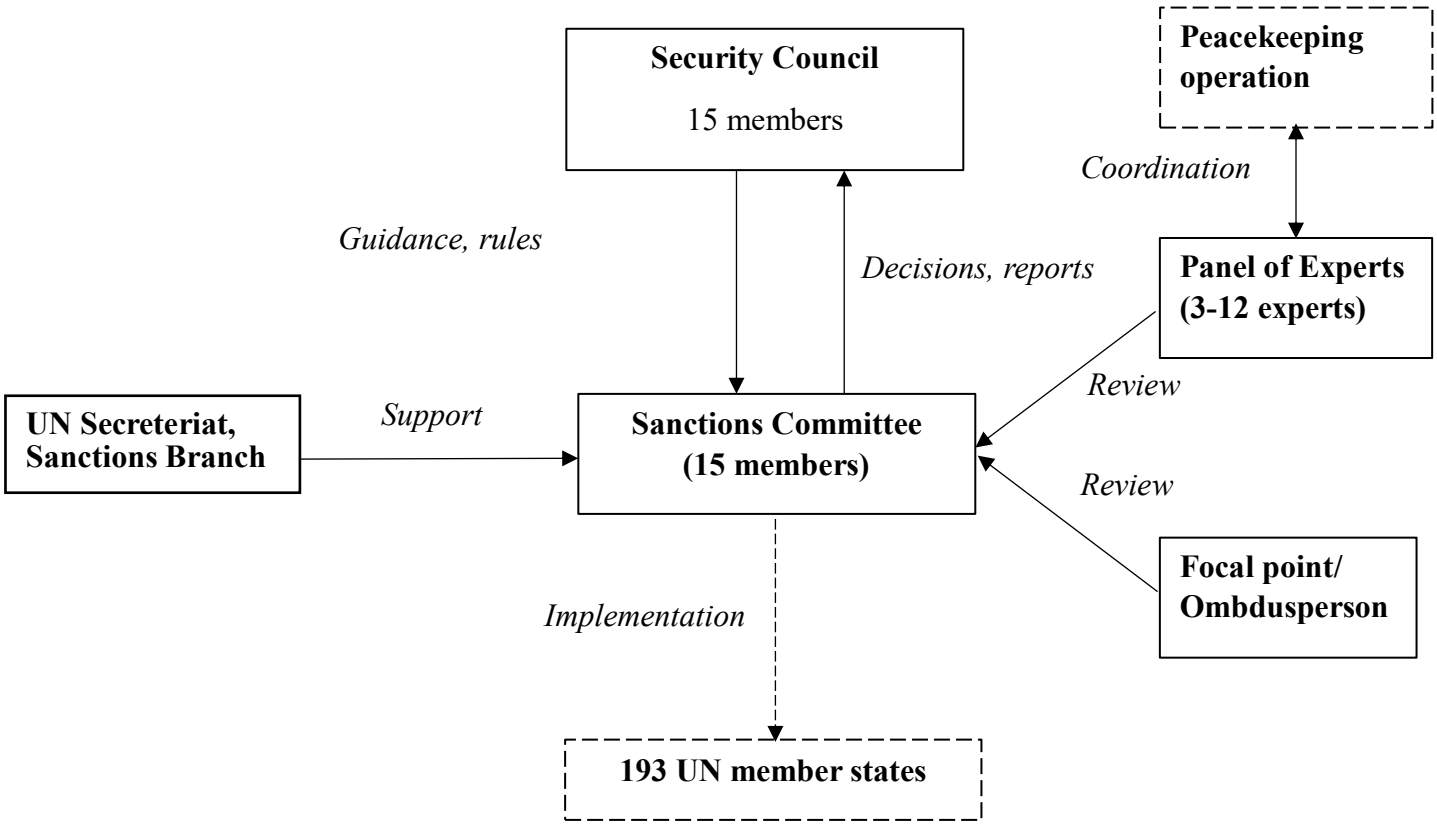


Figure 2.1 – The governance structure of Security Council sanctions regimes

Figure of own production; Source: Dorfler T. (2019), *Security Council sanctions governance: the power and limits of rules*. New York: Routledge.

2.2 Different types of sanctions: a historical analysis of the instrument and the evolution of its use before and after the cold war

Although the UN Charter contains many inventions, the difficulty of sanctions can't be counted among them. In fact, sanctions have existed since earlier period, although actions that don't involve the employment of force or military means. Famous, during this sense, is that the action of the city-state Aegina, which hijacked an Athenian ship and held the passenger's hostage. The action was a consequence of the non-release of several Aeginetan citizens who were being held captive within the current national capital. Without going too far back in time, the coalition born in city has, in fact, taken up, in some parts, the sanctions system of the League of states, improving its critical points. Indeed, the foremost notable improvement was the centralisation of decision-making, whereas within the League of states it had been left to individual states to choose whether to use sanctions. This was one in every of the best limitations of the League of states, which undermined its credibility. It is interesting to clarify the case of the economic sanctions against Italy within the context of the war in Ethiopia. Of the 50 states belonging to the coalition, none voted against the sanctions within the Assembly - there was a vote against by Italy and abstentions by Austria, Hungary and Albania - then again many of those maintained relations with Italy, supplying it with raw materials. This has been overcome by the already mentioned Chapter Seven of the Charter. Regarding the kinds of sanctions measures, the foremost used imposed at UN level are as follows:

1. Asset freezes
2. Arms embargoes
3. Commodity interdictions
4. Travel bans
5. Diplomatic sanctions

The security Council can value more highly to impose any combination of those measures within the framework of a personal sanctions regime.

- Asset Freezes

Most of the UN sanctions regimes that are currently operating incorporate targeted asset freezes of some kind. Resolution 1267 (1999), which ushered within the era of targeted sanctions, provides that each one Member States shall '[f]reeze funds and other financial resources, including funds derived or generated from property owned or controlled directly or indirectly by the Taliban, or by any undertaking owned or controlled by Taliban, as designated by the Committee'.Asset freezes usually operate by regard to an inventory of designated individuals and entities. These are the individuals targeted by the sanctions regime and whose assets

and property must be frozen. As with all UN sanctions measures, the imposition of asset freezes requires implementation and enforcement by individual Member States. However, in contrast to other more general trade restrictions, asset freezes offer little room for manoeuvre in terms of how Member States prefer to implement them domestically. specifically, the top result should be that the assets belonging to or controlled by the persons listed within the relevant UN sanctions committee list are frozen by Member States.

- Arms Embargoes

Again, most UN sanctions regimes operating contain arms embargoes, usually preventing the sale, supply or transfer of weapons to the territory or state that has been made the target of measures. Arms embargoes may target both conventional and unconventional weapons. within the case of the North Korean and Iranian sanctions regimes, the arms embargo provisions include specific non-proliferation measures. Moreover, arms embargoes can function as two-way prohibitions, targeting both the availability of weapons to a specific country and therefore the sale of weapons from or by the identical country. The latter is aimed toward depriving targeted governments of a key source of income.

- Commodity Interdictions

Commodity interdictions target commodities linked to conflict areas, or which are recognized as a key source of funds for governments targeted by sanctions measures. as an example, resolution 1643 (2005) in reference to the Ivory Coast prohibited the export of diamonds from that country. However, commodity interdictions feature far less prominently among the UN's sanctions regimes, partly thanks to the difficulties related to preventing avoidance, abuse and sanctions-busting. This was particularly the case in regard to the Oil-for-Food Programme in Iraq, which operated between 1995 and 2003 and provided for exceptions to the great prohibition on the export of oil from Iraq. The programme is widely considered to own been systematically manipulated by and for the advantage of the Iraqi Government.

- Travel Bans

Travel bans are another common sort of targeted sanction. like asset freezes, they operate by relevancy designated lists of people. as an example, resolution 1970 (2011), managing the case in Libya, calls upon Member States to 'take the required measures to stop the entry into or transit through their territories of people listed in Annex I of this resolution or designated by the Committee established pursuant to paragraph 24 below'.

- Diplomatic Sanctions

Article 41 of the UN Charter specifically refers to the 'severance of diplomatic relations' as a possible sanctions measure. However, whilst diplomatic sanctions were commonly utilized in the past, none are imposed in regard to sanctions regimes currently operating. this could appear to point that the safety Council is a smaller amount willing to forego the potential benefits of multilateral negotiations involving the targeted state as a method of resolving international conflicts[26]. Although sanctions were present in Chapter Seven of the Charter, only two cases of sanctions may be analysed during the Cold War: Republic of South Africa and Republic of Zimbabwe. These are the primary two mandatory sanctions regimes that the protection Council adopted and that they were built on the hope that UN sanctions would finally function a globally unifying and human rights- and norm-enforcement tool. That the member states of the NAM were the main factors behind the push for the primary two sanctions regimes, directed at Apartheid African nation and therefore the racist secessionists of Rhodesia, perceived to be a hopeful sign. This emerging global third force of the bulk, so far unrepresented people and countries of the planet, as a counter-balance to NATO and Warsaw Pact nations, signaled that perhaps now the struggle for consensus in SC politics would start. True, the imbalances in Council membership still needed to be resolved, and also the allocation of Taiwan's permanent Council seat to the foremost populous nation on earth, the Peoples Republic of China, was still years away. Nevertheless, under the leadership of India and also the first independent countries of Africa, the push for racial equality gave the impression to be a self-evident choice for crafting a winning global norm. However, the protection Council quickly taught the proponents of racial equality that democracy took a back seat to post-colonial interests and conflict gambits. Once vital body politic interests and sacrifices expected of them were exposed, meaningful actions against the Apartheid regime of African country and against the racist secessionists of Southern Rhodesia were quickly asphyxiated.

2.2.1 Apartheid South Africa

South Africa first received council attention in response to the Sharpeville massacre on 21 March 1960. South Africa's racist police had opened fire on thousands of individuals protesting the country's new Pass Laws that restricted the travel of black South Africans. The police in Sharpeville opened fire, using machine guns and armored vehicles, supported by military helicopters and jet fighters. Sixty-nine people, including women and youngsters, all black, were mowed down and lots of others were injured. Subsequent investigations revealed that a number of the victims had bullet wounds within the back, having been shot while fleeing, instead

[26] Gordon R. J. F., Smyth M., Cornell T., (ed.), (2019), *Sanctions law*. Oxford, UK; Portland, Oregon: Hart Publishing.

of attacking, because the police alleged. Despite the outrageous and disproportionate use of force, a transparent violation of long-established international humanitarian law, most Western countries resisted the decision by African and NAM (Non-Aligned Movement) member states for the protection Council to intervene in an exceedingly serious manner against South Africa's Apartheid regime. During the conflict, the supremacist regime of Republic of South Africa was considered NATO's most significant strategic sub-Saharan ally. As a part of country Commonwealth, it actively operated as a belligerent proxy force against socialist-leaning neighbor states. South Africa had also, with the assistance of Israel, developed nuclear technologies even past the so-called Vela incident that a lot of suspected was an undeclared test detonation of a nuclear device. The Sharpeville massacre, however, significantly increased pressure from African and NAM member states, led by India. Fourteen years later, after Sharpeville, India initiated a decades-long campaign through which it exposed the Apartheid regime and attempted to garner the support of Western states, including the P3 within the SC. along with 29 other states, India submitted a proper complaint to the protection Council to which, after much internal wrangling, the protection Council responded with its first resolution associated with Apartheid African nation, the Resolution 134/1960. Despite this painfully watered-down decision—abstained by France and also the UK—the council set variety of important precedents. In paragraph 1, it stated that true has "led to international friction and if continued might endanger international peace and security".

Under paragraph 5, it also acknowledged that the administrator and African nation should make arrangements as would "adequately help in upholding the needs and principles of the Charter". But the underside line was that the Western countries' thinly disguised bias against the victims of racial violence prevailed and no binding sanctions resolution against Apartheid South Africa was adopted. this may remain the pattern for the approaching decades. In 1963, in response to the continued escalation of violent racism and new complaints by African and NAM member states, the Council adopted its first voluntary sanctions resolution – Resolution 181/1963 - prefacing its decisions with the observation that "the situation in South Africa is seriously disturbing international peace and security." The resolution "strongly deprecates the policies of Republic of South Africa in its perpetuation of favoritism as being inconsistent with the principles of the UN and contrary to its obligations as a member of the global organization." Under paragraph 3, the resolution solemnly calls upon all states to "cease forthwith the sale and shipment of arms, ammunition of every type and military vehicles to African country." The resolution – Resolution 181/1963 – adopted in August 1963, justified this first-ever sanctions measure by noting that South Africa's arms buildup was partly accustomed further its apartheid policies. In December 1963, the safety Council adopted another resolution – Resolution 182/1963 – requesting from the Secretary-General the establishment of a "small group of recognized experts to look at methods of resolving this situation in Republic of South Africa through full, peaceful and orderly application of human rights and fundamental freedoms to all or any inhabitants of the territory as a full, no matter race, colour or creed,". The Group would subsequently be called the "Group of Experts" and while its

first report didn't recommend the imposition of sanctions, it did recommend that the safety Council examine the economic and strategic aspects of sanctions. In June 1964, the protection Council concurred with key points of the Group of Experts report, with Resolution 191 mandating the establishment of an expert committee to review the feasibility, effectiveness, and implications of measures which can be taken by the Council under the Charter of the global organization. It also commissioned the Secretary-General to determine an academic and educational program because the Experts had recommended, albeit, much more modest in ambition, and even more so in funding. In 1976, tensions rose again in African nation in response to the Soweto Uprising. Commencing on 16 June, between 10,000 and 20,000 students protested in response to Government-imposed language laws requiring the employment of Afrikaans within the college system. Police reaction to contain revolting students quickly spiraled out of control and therefore the photos and reports of dead youth shot and killed by police were plastered across the front page of the many newspapers of the planet. Within days, the protection Council condemned the violence and killings of faculty children and over the subsequent months the massacre prompted increased international attention. Norway and Sweden became the primary Western countries to impose partial economic sanctions on Republic of South Africa.

At the UN, the final Assembly drafted a lengthy and detailed Programme of Action against Apartheid that outlined measures to further isolate South Africa. After the Soweto Uprising, public pressure and global scorn for South Africa's racist policies increased, making it politically untenable for the governments of Western supporters to tolerate and covertly support Apartheid politicians. On 4 November 1977, the protection Council finally adopted mandatory sanctions measures (Resolution 418/1977). The arms embargo on African country required all states to stop the sale or transfer of arms or related material, including military or paramilitary vehicles and equipment, spare parts, or the granting of licenses for the manufacture of the above. Concerned about South Africa's nuclear arms proliferation, the Council also prohibited all states from assisting Republic of South Africa within the manufacture and development of nuclear weapons. the subsequent month, the safety Council authorized the formation of the 418 Sanctions Committee (Resolution 421/1977).

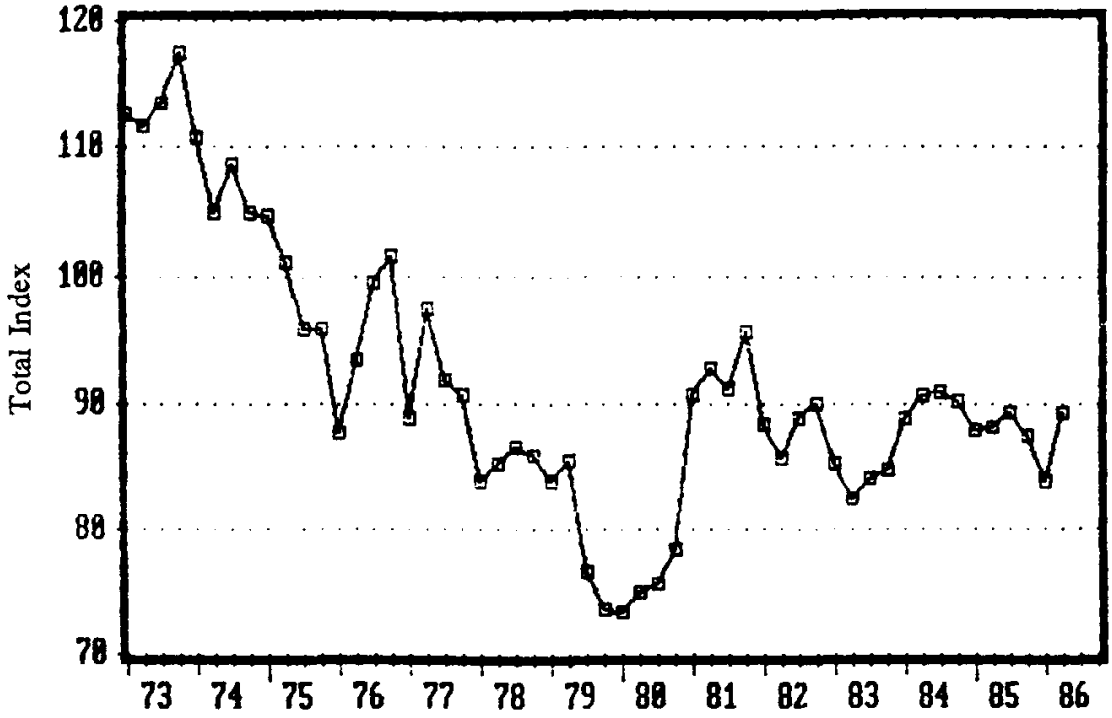
Notwithstanding intense lobbying from British unions, and a student campaign for his or her university endowments to disinvest from all companies doing business for, with, or in African nation, the deteriorating reputation of the Apartheid regime never led to stronger UN sanctions. a crucial a part of the globe community's modest resolve and actions was renewed conflict tensions. In support of their aggressive global anti-Soviet strategy, the US administration of United States President and therefore the UK government of Margaret Thatcher revived their countries' traditional tolerance for the Apartheid regime. Apartheid African country served as an anti-communist bulwark within the war against Russian-Cuban meddling within the civil wars of Angola and Mozambique. An important motivation for growing global attention was the plight of South Africa's political prisoners. besieged from NAM and African member

states, the safety Council had called as early as 1964 upon Republic of South Africa to renounce executions, death sentences, and imprisonment of the opponents of apartheid (Resolutions 190/1964 and 191/1964). Nelson Mandela, serving immurement since his arrest in 1962, came to symbolize both inside and outdoors African nation the long struggle against apartheid and racism. By 1980, the Free solon campaign had mobilized anti-apartheid proponents globally to which the protection Council responded with a symbolic require the discharge of Mandela and every one other political prisoners, in Resolution 473/1980. The accumulating global pressure likewise because the economic isolation of South Africa, while facing the requirement to fulfill rising costs for its internal security and paramilitary forces, gradually convinced even conservatives within the National Party that the Apartheid policies were now not a sustainable way forward. Internal tensions forced South Africa's President P.W. Botha to resign as leader of the National Party in February 1989 and represent elections against Frederik Willem de Klerk, the leader of the Transvaal branch of the Party, known to be the foremost conservative within the country. But de Klerk had already taken the lead among the "verligte," Afrikaans for the enlightened flank of the party and, thus, was elected the new President of the country. Within weeks, he initiated secret negotiations with solon, and by February 1990 released him, and lifted the ban on the ANC also as other liberation movements. Effectively, the target of the 118/418 sanctions regime was now met and theoretically, it could are lifted. The opening of the South African orbit revealed deep cleavages, some with pre-colonial histories, among South Africa's native nations. The Zulu, the most important and most influential ethnicity, were internally divided between a moderate majority to which belonged much of the ANC leadership, including Nelson Mandela, and a separate group led by Chief Mangosuthu "Gatsha" Buthelezi, called the Inkatha FTO. Originally pursuing very similar goals and techniques, Chief Buthelezi gradually deviated from ANC policies, specifically when he began to advocate non-violent protests. Once De Klerk began to dismantle apartheid policies, the Inkatha agitated for autonomous status for his or her traditional KwaZulu-Natal region that had already been claimed by the founding father of the group, Zulu King Solomon kaDinuzulu. so as to secure their objectives, Buthelezi increasingly engaged directly with the leaders of the National Party. But tensions grew when information leaked to the general public about covert funding and arms supplies from the South African Defense Forces to support Inkatha and Buthelezi against the ANC. Between the time when Mandela was released from prison on Robben Island, the adoption of a brand new South African Constitution, and national elections, violence erupted between the Inkatha and ANC, often leading to several deaths. At the identical time, extremists of the National Party splitting off to make racist groups, and vindictive black activists, also meted out retributive violent acts against one another. With a devastating surge of violence gripping African country, the protection Council decided to take care of the sanctions regime with Resolution 765/1992 and to determine the UN Observer Mission in Republic of South Africa (UNOMSA) with Resolution 772/1992. De Klerk's political pivot also led to the cessation and eventual dismantling of South Africa's proliferation program. South Africa had stepped back from its military aggression against neighbors, having already in 1988 ended its

involvement within the warfare of Angola and now it might also refrain from other adventures in Mozambique, and Zimbabwe. With the collapse of the country during the 1989–1990 period, South Africa's strategic position within the world radically changed also. As an expression of its new regional policies, African nation became a signatory to the Non-Proliferation Treaty in 1991. After the 27 April 1994 election that made Nelson Rolihlahla Mandela the primary black President of Republic of South Africa, it became a number one regional mediator and a force for peace. the safety Council terminated the arms embargo and other restrictions on 26 May 1994 (Resolution 919/1994). On 27 June 1994, the Council terminated UNOMSA and declared that the UNSC was now not seized of the matter of African country (Resolution 930/1994). In conclusion, over a period of 12 years, the sanctions regime against apartheid successfully coerced South Africa's racist leadership into changing its policies and served as a point of interest for a growing political public campaign. Increasing political will in many countries forced the regime to open a path to black philosophy.

However, these sanctions-induced developments are marred forever, within the eyes of most Africans and other residents of former Western colonies, by the 17-year-long resistance by France, the UK, and therefore the US to taking a meaningful stance against the human rights violating Apartheid regime. Student and union movements in these countries during the 1980s became vocal anti-apartheid forces. But their activism came twenty years too late and left little confidence within the commitment of the governments of those Western lead nations to the UN and its humanitarian values[27]. Below a graph for example the effectiveness of the sanctions regarding trade.

[27] Carisch E., Rickard-Martin L., Meister, S. R. (2017), *The Evolution of UN Sanctions From a Tool of Warfare to a Tool of Peace, Security and Human Rights*. Springer International Publishing AG.



Note: Terms of trade equal export prices divided by import prices.
Source: International Financial Statistics, IMF.

Figure 2.2 Values of trade during the sanctions period in Apartheid South Africa

As we will see from the graph, trade sanctions are likely to be ineffective due to the substitutability of goods and also the fungibility of markets. whether or not most or all countries coordinate actions against the target country, this suggests that the gain from surreptitious cheating by individuals within the countries applying sanctions are going to be great. Therefore, one may view the economic damage to the target country not as making that country do without trade but as worsening its terms of trade: the worth of imports rises relative thereto of exports. Initially, we specialize in the terms of trade, or the value of a country's exports relative to it of its imports. This represents a country's purchasing power on world markets. Figure 2 illustrates the continual decline of South Africa's terms of trade throughout the 1970s and shows some rebound during the 1980-1981 period, when oil prices returned to pre-1979 levels and gold prices rose on world markets. The South African terms of trade have remained relatively stable throughout the 1980s. The economy of South African ultimately remains tied to commodity exports-namely precious metals. This group of commodities-largely gold but including diamonds and other metals-helps isolate the South African economy from serious terms of trade deterioration caused by economic sanctions[28].

[28] Kaempfer W. H., Moffett M. H. (1988), "Impact of anti-apartheid sanctions on South Africa: some trade and financial evidence", *Contemporary economic policy*, Volume 55, Issue 4, pp. 118-129.

2.2.2 Southern Rhodesia

The breakup of the British controlled but self-governing Federation of Rhodesia and Nyasaland—encompassing a territory roughly adequate today's Zimbabwe, Malawi, and Zambia—was driven in large part by the strengthening black independence movements. While future leaders prepared to require over their countries, partly supported by a people government, the white minorities of the Federation focused on preserving their control over the economically most viable African nation. When the Federation dissolved, first with the independence of Nyasaland (Malawi) in January 1964, followed by Zambia during the subsequent October, African nation remained a British colony whose white-minority population failed to want to undergo the black majority. Commonwealth rules dictated that the United Kingdom didn't release former colonies into independence without their meeting the "No Independence Before Majority African Rule" (Minter & Schmidt, 1988). For this reason, it had been considered untenable to permit the white minority to rule over the vast black majority of African country without triggering uncertainties and protests throughout land Commonwealth. This decision, however, didn't sit right with the Rhodesian Front, the white, party led by Smith, a populist career politician. The considerable governing privileges of the Rhodesians allowed their Rhodesian Front party to introduce many racist laws and discriminatory land appropriations similarly as impose severe restrictions on political freedoms and activities of the non-white population. Southern Rhodesian independence first received attention within the General Assembly in 1962 in response to adoption of the 1961 Constitution of Southern Rhodesia which firmly placed control of the territory with the white minority. In response, the final Assembly condemned during a resolution the denial of rights to the bulk and called upon the United Kingdom to require several actions to resolve matters. Britain vetoed a draft resolution within the SC that will have invited it to not transfer to Rhodesians "any powers or attributes of sovereignty until the establishment of a government fully representative of all the inhabitants of the colony" (Resolution 181/1963). Two years later, the Rhodesian Bush War broke out between the black majority and therefore the white minority and, by 1965, things on the bottom had intensified, particularly because of increased threats by the Rhodesian Government to interrupt from the United Kingdom. Smith becoming Prime Minister in 1964 further exacerbated tensions, particularly when he imposed a ban on all black separatist movements, targeting the Shona-dominated Zimbabwe African National Union (ZANU) and also the Zimbabwe African People's Union of the Ndebeles. In response to requests from the United Kingdom, the overall Assembly, and its Special Committee on Decolonization, the protection Council issued its first Resolution on the Southern Rhodesian situation (Resolution 202/1965). The immediate trigger was the government's adoption of a racist constitution and announcement of elections to require place in May 1965. Mirroring the final Assembly, SC Resolution 202 requested that the United Kingdom "take all necessary action" to stop Rhodesia's breakaway; called upon member states to not recognize an independent Rhodesia if it should perform its threat; and called upon the United Kingdom to figure with the Rhodesian

Government to make a brand-new inclusive constitution. Although condemning the actions of the illegal authority on the bottom, both the UNGA and therefore the Security Council made it clear that the problem of Southern Rhodesian independence was the responsibility of the united kingdom to resolve.The UK was to intervene to form conditions for the convening of a constitutional conference, to stop the unilateral declaration of independence (UDI) of African nation, and to make sure that school of thought would be established.

Notwithstanding the protection Council's and therefore the British government's demands, solon and his Rhodesian Front-dominated cabinet issued a UDI in November 1965. With this act, Smith and therefore the white minority forced the hand of the international community, upset British decolonization policies laid out by British Premier Minister Harold Macmillan's February 1960 Wind of Change speech, and threatened African nationalism, which had become the continent's dominant philosophy for regime change.

In the immediate aftermath, the safety Council first adopted Resolution 216 condemning the declaration of independence and calling on all member states to not recognize the regime. some days later, Resolution 217 spelled out the terms of what was essentially a voluntary arms embargo likewise as comprehensive economic sanctions (Resolution 217/1965). the 2 resolutions failed to, however, satisfy strong sanctions advocates among African and NAM states, who in parallel with their mobilization against African country's Apartheid regime, now also demanded strong measures, including military intervention by the United Kingdom and other countries, so as to prevent the racist regime in Salisbury (today's Harare). a people government had, however, excluded group action as an option, leaving imposition of an embargo as its only viable alternative.

Resolution 217 again declared the racist minority's declaration of independence illegal, and therefore the council called upon all states to ban diplomatic relations with the illegal authority. States were also called upon to stop actions that will support the authority, particularly to ban the availability of arms, equipment, and military material. Furthermore, they were to interrupt off economic relations with African country to the most effective of their ability, including the implementation of an oil and petroleum embargo. the United Kingdom was again given primary responsibility for resolving matters and taking all measures necessary to eliminate and end the illegal government. Additionally, under Chapter 8 of the UN Charter, the Council called upon the OAU (Organisation of African Unity) to help in implementing the resolution. During the meeting following the vote, several members noted that the measures weren't strong enough, nor could the members effectively implement all of them. This successfully convinced the protection Council to amplify the measures by issuing a further statement by the President of the safety Council. The British Navy was to intercept select imports and exports originating from or destined to Rhodesia that felt the Mozambique Channel, the body of water between the African coast and therefore the geographical region of Madagascar. country government, still hoping to be able to lure the secessionists back to the colonial fold, preferred however to use its general trade restrictions only selectively together with a ban on oil exports to Rhodesia. While debates played call at nation Parliament about the acceptable severity of embargo enforcement to bend the desire of the Salisbury secessionists, the leaders in Rhodesia dug in their heels and settled certain the long-standing time. African

nation had replaced Mozambique within the refinement and delivery of oil to Southern Rhodesia, eventually using land transportation through the building of a railway link to permit direct delivery. Fully tuned in to the circumvention scheme, the United Kingdom was unwilling to watch the waters off Republic of South Africa. Its officials let it's known that this extra act would be viewed as a provocation. In light of violations of the oil embargo and therefore the undeniable fact that voluntary measures weren't having the required effect, African and NAM member states lobbied hard for the safety Council to adopt its first mandatory sanctions (Resolution 232/1966). Although some measures like the prevention of monetary or other gift to Rhodesia remained voluntary (Resolution 221/1966), preventing the importation of variety of specific items from African country; trading in or engaging in activities that promoted the export of the many natural resources and commodities from Rhodesia; and also the sale or shipment of arms and related equipment or materials for the manufacture of arms and ammunition in Southern Rhodesia, were mandatory sanctions measures. Member states were also to dam the availability of aircraft and cars and related equipment, and stop the shipment of such goods via vessels and aircraft destined for African country. Restriction of the availability of oil or oil products to Rhodesia was now mandatory. Bulgaria, France, Mali, and Russia abstained from the vote to adopt Resolution 232. Despite those violations of the sanctions were soon widely known, the protection Council failed to revisit the Southern Rhodesian issue for an additional 18 months. The new resolution expressed the Council's concern that measures taken to date had "failed" to resolve the difficulty in Rhodesia and furthermore, expressed its concern that not all states had complied with the measures. The warfare was also taking its toll and also the Council condemned the executions disbursed by the illegal authority. Adding way more detailed descriptions to its embargo measures, the Council again enacted mandatory trade restrictions on all imports from Southern Rhodesia; and required that member states prevent any activities associated with promoting exports from the Rhodesian territory, transportation of embargoed goods via ships or aircraft, and also the sale or supply of embargoed goods by nationals of member states or within their territories, no matter origin, to anyone in Republic of Zimbabwe or for any business operating out of Republic of Zimbabwe. States were also to use financial sanctions on Southern Rhodesia, apart from payments associated with humanitarian or educational purposes, in addition as a travel ban on Southern Rhodesians and a flight ban on aircraft from its territory.
The Council also requested member states to require any longer actions possible under Article 41, i.e., additional sanctions against the state. The Council also authorized its first sanctions committee, the 253 Committee, to look at reports by states sent to the administrator on the implementation of the sanctions and to watch trade with Republic of Zimbabwe further as sanctions evasion. Although the primary SC sanctions committee operated under restraints imposed by a number of the P5, it absolutely was able to report on compliance and infrequently detect violations of the sanctions regime. for example, the Committee's July 1970 report discerned those exports of chrome ore from African nation didn't match import reports from other countries, particularly South Africa—which it surmised was importing significant quantities of the mineral. A

year later, provided that chrome ore was a significant export commodity for Southern Rhodesia, it had been added to the embargo in Resolution 314/1972. Although the Council supported other Committee recommendations, countries continued to violate the sanctions. The US—which the Council sometimes called out for its sanctions violations directly within its resolutions—openly authorized the importation of chrome ore soon after the embargo, or allowed national leader and other members into the US in violation of the travel ban. Following Resolution 277/1970, states were to sever all diplomatic ties with African country, and therefore the Security Council requested that Rhodesia's membership within the UN and other international institutions or organizations be suspended. the protection Council began to admonish South Africa and Portugal for his or her complicity in aiding African nation in reference to the white-minority regime in South Africa—itself under voluntary sanctions for its apartheid policies and activities, but the reprimand had no effect. The Council demanded that African country withdraw its police and other personnel it had deployed to Rhodesia, which was an instantaneous violation of the 277 sanctions. A draft resolution proposed the day before Resolution 277 was adopted—which proposed secondary sanctions on Portugal and Republic of South Africa and condemned the United Kingdom for not using force against the racist secessionists of Rhodesia—was vetoed by the US and UK. In the latter half the 1970s, the illegal regime in Southern Rhodesia began to feel pressure from many quarters that may eventually force it to reconsider its independence under white-minority rule. When Southern Rhodesia's neighbor Mozambique and Angola both achieved independence from Portugal in 1975, Smith's government lost the strategically important support from these former European colonies who now supported Rhodesia's black majority. Additionally, South Africa, upon which African country had become increasingly reliant thanks to the UN and other international sanctions, began to withdraw its support from the illegal regime. the United Kingdom had threatened Republic of South Africa with international sanctions if it failed to sever ties with Smith's government. Internally, Zimbabwe was handling increasing violence and therefore the costs of a chronic war. Mounting losses plus the removing of important regional support allowed the sanctions to own a stronger impact. Smith's attempts in 1978 and 1979 to allot more authority to black Africans by revising the constitution again and holding an election that led to Southern Rhodesia's first black Prime Minister, Bishop Abel Tendekayi Muzorewa, didn't satisfy the international community. Members of the Southern Rhodesian government and rebel leaders, among others, met under British guidance and negotiated the 1979 Lancaster House Agreement which outlined a replacement constitution for independence, initiated a cease-fire, and led the thanks to elections. In response to the Agreement, the Council adopted Resolution 460 on 21 December 1979, which terminated the sanctions and dismantled the 253 sanctions regime. a touch over a month later, the safety Council noted violations of the Lancaster Agreement and issued Resolution 463/1980, calling upon the United Kingdom to make sure that free and fair elections transpire. An election in February 1980 brought Robert Mugabe—leader of the Zimbabwe African National Union—Patriotic Front (ZANU-PF), one in every of the rebel groups of the civil war—to power. Zimbabwe gained its independence in April and also the UN

accepted the country as a brand-new member in July (Resolution 477/1980). Great symbolism is attached to the UN's first mandatory sanctions regime. It should have served to support the UN's humanitarian principles against the racist regime of African nation. Yet the self-interested politics of the protection Council converted this issue to sanctions that targeted secessionism detrimental to a P5 member state, instead of assisting the discriminated population of Rhodesia. Thus, the urgent humanitarian rescue of voluminous black dissidents—incarcerated, tortured, and executed—became a political football for Whitehall's desktop generals. Weak implementation of the UN and British sanctions, along with overly tolerant handling of the racist secessionists unnecessarily prolonged the independence struggle. When finally, the results of sanctions along with pressure on the battlefield during the intensifying armed struggle for independence by ZANU/ZAPU fighters led to a sovereign majority government, the insurgents had turned against each other and extended the amount of national instability instead of facilitating a real national reconciliation of all Rhodesian actors, lackadaisical policies and sanctions practices fostered new hostilities and gave thanks to Robert Mugabe's strong man politics. In 1983, tensions between Mugabe's Shona majority and Nkomo's Ndebele population were renewed violent conflicts. Elite North Korean-trained Shona forces annihilated resisting Ndebele groups in Matabeleland and also the Midlands. The legacy of flawed decolonization policies, supported by UN sanctions, left Zimbabwe throughout its young history teetering on the brink of war[29].

2.2.3 The end of cold war and the beginning of a new era: from comprehensive to targeted sanctions

Until the mid-1990s, most UN sanctions were comprehensive. This was the case for Iraq, for Haiti and for many of the previous Yugoslavia. The underlying logic was to weaken the economy of a state so as to force the govt. of the day to vary its policies. Today, most sanctions are targeted, and their logic is to maximise the impact on the responsible individuals (in other words, the elite) within the country concerned, while minimizing humanitarian consequences for the innocent population. The evolution from one form to the opposite has occurred over a period of some 20 years, changing the UNSC's sanctioning practice and altering the prevalent view of the aim served by sanctions in diplomacy. Three major factors prompted the shift towards targeted sanctions. First, sanctions had gained a negative reputation internationally. leader failed to leave power as a consequence of UN sanctions; and therefore, the case of Rwanda epitomized not only the failure of the UNSC to act effectively, but also the impotence of sanctions when it came to handling the instabilities typical of the post-Cold War world. Second, sanctions against states seemed not only to be ineffective in changing regimes, but even to entrench in power the groups they were intended to undermine. Saddam Hussein's position was made not less but safer by sanctions, while in Haiti the junta managed to

[29] Carisch E., Rickard-Martin L., Meister, S. R. (2017), *The Evolution of UN Sanctions From a Tool of Warfare to a Tool of Peace, Security and Human Rights*. Springer International Publishing AG.

extend its power by running the illegal marketplace for sanctioned goods. Finally, sanctions were hurting innocent civilians over the elites whose behaviour the measures sought to change. The widespread view, subsequently reinforced by reputable reports, that 500,000 Iraqi children died as a results of UN comprehensive sanctions itself rang the death knell for the perceived utility of comprehensive measures. The evolution towards targeted sanctions was facilitated by the emerging principle of individual international responsibility. In essence, individuals were increasingly held in control of their actions; and then, while leader himself wasn't specifically targeted with sanctions in 1990, he was in 2003. Likewise, Muammar Gaddafi wasn't sanctioned within the 1990s, but was in 2011. Sanctioning heads of state represented a radical change in UN practice. the bottom was prepared by the creation within the 1990s of Special UN Criminal Tribunals (for example, to cater to the cases of Republic of Sierra Leone, Somalia, Rwanda and also the former Yugoslavia) and in 2002 of the International Court. By the 2000s, holding individuals responsible before the international community had become a norm, instead of the exception. The stage was set for sanctions to vary. There are theoretical instruments that are applicable to both the great and therefore the targeted versions of sanctions. for example, the controversy on the objectives of sanctions exists for both forms. Nearly 30 years ago, James Lindsay suggested a typology with five objectives that's applicable to any sanction. The more moderen typology of how sanctions work—namely, whether sanctions coerce, constrain and/or signal—is also applicable to both comprehensive and targeted sanctions. Whether targeted or not, sanctions will be punitive measures, and will be considered the simplest policy option at a selected time. Both comprehensive and targeted sanctions can provoke the 'rally-round-the-flag' effect within the target state, and both forms can have humanitarian consequences. The impact of sanctions, if measured at a macro level (e.g., GDP growth, inflation, etc.), is another useful variable in comparing comprehensive sanctions on the one hand and targeted sanctions on the opposite. Targeted sanctions are in no way problem-free. for example, there's a full of life debate within the literature on the legal challenges to which they provide rise. Targeting individuals and non-state entities creates tensions with other principles established in international treaties, like those of group action and effective remedy. the utilization of targeted sanctions to counter terrorism raised particular concerns about human rights violations in sight of the way during which individuals were added to the lists of these to be sanctioned. The national implementation of UN sanctions has also been discussed, as has the unevenness of state capacities to confirm that targeted sanctions are given effect. Finally, whereas the difficulty of effectiveness is after all a central topic for sanctions normally, there has been a discussion on whether targeted sanctions are more or less effective than comprehensive sanctions, marking the difference between the 2 when the dominant narrative had didn't acknowledge it. Targeted sanctions are designed to maximise the impact on responsible individuals and minimize consequences for innocent civilians, but what does that mean in practice? Who are the targets? When should the UNSC use sanctions? How innovative has the UNSC been in designing and implementing new sanctions? The targeted sanctions consortium's empirical analysis of UN sanctions offers the chance to spot and examine the distinctive elements of targeted

sanctions, because the next section will demonstrate. Targeting non-state actors isn't the identical thing as sanctioning states. this is often the driving logic behind the formation of the TSC (Targeted Sanctions Consortium) and therefore the decision to form a comparative and comprehensive database of all UN targeted sanctions for a complete of 23 cases and 63 episodes. The expectation of these fitting the TSC database was to gather evidence and identify patterns or features from cases of targeted sanctions that differ from those apparent in cases of comprehensive sanctions. The TSC database uses 296 variables grouped into 15 categories. Regarding this work, three categories are particularly relevant: the objectives, the targets and also the variety of measures applied. The first category concerns the objectives of sanctions. Although this category will be accustomed study comprehensive sanctions moreover, the adoption of targeted sanctions facilitated the expansion of the range of circumstances within which sanctions may well be applied, and therefore the range of objectives that might be pursued. Comprehensive measures targeted states, and were originally intended as an instrument of peace to use as another to war. In contrast, targeted sanctions operate at the intrastate level, and that we may therefore expect to work out such sanctions being employed to deal with a range of various forms of crises. Targeted sanctions regimes may be altered quite easily—for instance, by adding names to lists or removing them, adding exceptions, widening or narrowing targeted trade sectors—and this flexibility facilitates their expansion into areas not previously subject to sanctioning, a minimum of not by the UN. Empirical analysis of the UN experience sheds light on when and the way targeted sanctions are used and creates opportunities for brand spanking new areas of sanctioning activity within the future. The UNSC has interpreted Chapter VII of the Charter in numerous ways within the past twenty years, enabling a more frequent use of targeted sanctions. The TSC identifies nine varieties of situation during which UN targeted sanctions are used. people who appear most often are efforts to finish hostilities and to enforce peace within the context of armed conflict, each of which applies to about 49 per cent of the sample.

Table 2.2 – Distinctive features of targeted sanctions: objectives and targets

When applied: objectives	**No. of episodes**	**To whom/what applied: targets**	**Primary target (%)**	**Targets (%)** *
Cease hostilities	49	Entire government	19	59
Peace enforcement	49	Government leadership	25	53
Human rights	35	Rebel faction	25	43
Democracy support	27	All parties	16	29
Counterterrorism	24	Terrorist group	1	10
Peacebuilding	16	Leadership family members	0	22
Good governance	13	Facilitators	2	31
Support negotiated peace agreement	13	Individual targets	1	45
Support judicial process	10	Key regime supporters	0	14
Support humanitarian effort	6	Domestic constituencies	1	7
Responsibility to Protect	3	Regional constituencies	6	25
		Global constituencies	4	16

* Average of coercing, constraining and signalling.

Targeted sanctions, then, are used not only in wars between states but also in intrastate situations, like post-conflict management and judicial processes deemed to want support. this is often a big change in practice for the safety Council, representing an extension of interest from interstate relations into matters internal to states. The range of crises within which sanctions are applied reflect the various objectives that targeted sanctions are intended to attain. The second category of variables of interest to targeted sanctions concerns the kinds of target at which sanctions are directed. because the great majority of targets of sanctions are now individuals and non-state entities, the understanding of how sanctions work must be adjusted to the current new reality. Sanctions are often, but not always—or even most frequently—directed at the govt and its members. The TSC distinguishes ten target categories that don't include the national government, like rebels and relations of targeted individuals. The dataset also distinguishes between primary and secondary targets—primary targets are those that concern the foremost senders, while secondary targets suffer sanctions thanks to their reference to primary targets—a distinction that offers rise to a number of the foremost interesting conclusions. The main finding is that the whole government is that the primary target of sanctions in 19 per cent of cases—for instance, those of Liberia and Côte d'Ivoire—and some of its members (such as senior military leadership) in 25 per cent of cases. this suggests that the govt. as a full or its members are targeted in under half all cases. The proportion of cases involving governments goes up to 55 per cent if secondary targets are included: this, for instance, brings within the cases of Kosovo, Rwanda (in the first phase) and therefore the Central African Republic. Sanctions are frequently aimed toward rebel factions, which were targeted in 25 per cent of episodes from the database, for instance in Angola, African nation, the Democratic Republic of Congo and therefore the Taliban in Afghanistan after 2001. Such groups are often tougher to handle than governments and are less likely to compromise with the stress of the international community. Again, the proportion rises (to 43 per cent) if secondary targets are included, which brings within the latest episode of sanctions against Somalia and also the first episode against Rwanda. Accounting for secondary targets becomes central to the analysis when sanctions directed at intermediary actors acquire play. These intermediaries, who may have links with peace 'spoilers', for example those that try and break a peace settlement once achieved, include relations, facilitators and key regime supporters. Such figures are frequently subjected to sanctions, though they're less likely to be the first targets. Overall, intermediaries feature during a quarter of cases within the dataset, starting from 10 per cent of terrorist groups to 45 per cent of individual targets (which includes also non-state entities like firms). The third category regards the kind of sanctions imposed. As targeted sanctions offer opportunities for institutional innovation, the UN provides a decent case-study, offering the possibility to research how sanctions have evolved over time and what sorts of measures are used. The TSC dataset provides this information within a conceptual framework that may be accustomed make comparisons between cases and over time. The UN has imposed a large range of individual, sectoral and territorial sanctions. Generally speaking, the foremost commonly used type is that the sectoral ban, which is imposed in 95 per cent of the cases (e.g., arms embargoes). The second most

frequent style of sanctions comprises measures against individuals, like travel bans (75 per cent) and asset freezes (63 per cent). the smallest amount frequently used category is financial sanctions applied against a government, which are employed in only 10 per cent of the episodes[30]. In conclusion, is vital to undertake to analyse impacts and effectiveness of targeted sanctions. Despite most of the cases analysed by this project are ongoing and therefore the information on impacts is incomplete in many episodes, there are some interesting connections.

Table 2.3 – Effectiveness by purpose and type of direct impacts

	Type of direct impact			
	Psychological	Political	Economic	All impacts
Effectiveness by purpose	Frequency	Frequency	Frequency	Frequency
Effective: Coercion (5)	0/2	1/5	0/3	1/10
Effective: Constraint (16)	0/8	3/15	1/12	7/10
Effective: Signalling (17)	0/9	3/15	1/12	8/10
Ineffective (39)	0/6	8/13	7/12	2/2

Table of own production; Source: Biersteker T. J., Tourinho M., Eckert S. E. (ed.), (2016), Targeted sanctions: the impacts and effectiveness of United Nations action. New York: Cambridge University Press.

The table shows the sort of direct impacts related to effective sanctions by purpose, and for ineffective sanctions overall. First, psychological impacts alone are never related to any degree of sanctions effectiveness. Episodes where all three kinds of impact are present were effective, usually for constraining and signalling, all told but two episodes (Iran and Côte d'Ivoire within the last episodes). And these episodes, not surprisingly, involve a large type of sanctions. All combine sectoral, commodity, or financial sanctions with the more targeted arms embargoes and individually targeted measures. Political or economic impacts alone seldom correlate with effectiveness. A major contribution of the TSC research is that it systematically analyses every type of targeted sanctions, not just economic measures. It also analyses political and psychological impacts, alongside economic ones. this is often important because some targeted sanctions, as an example, travel bans, will have little if any economic impact in targeted countries. At the identical time, it seems to be a challenge to assess the impact of various targeted sanctions because they're rarely utilized in isolation. A few interesting associations do emerge from the info. One is that the case studies suggest that psychological impacts are relatively uncommon, even when sanctions publicly and prominently target individuals. But it's not clear whether that's because these impacts really are rare or because they're extremely hard to look at. It could even

[30] Giumelli F. (2011), *Coercing, constraining and signalling: explaining UN and EU sanctions after the cold war*. Colchester: ECPR press.

be because terrorists, coup leaders, and human rights abusers are difficult to embarrass. The evidence also suggests that the more narrowly targeted sanctions – individual travel bans and asset freezes, and arms embargoes – typically have fewer impacts than other types and barely involve economic impacts. Episodes involving broader sanctions that affect important economic sectors or commodities lead to more impacts and unintended consequences; the sanctions in those episodes appear to be more practical at signalling and constraining targets. to form more definitive judgements in these areas, however, the research will must further assess the relative magnitude of the impacts. Finally, this work only touches the surface of issues that are possible to analyze using the info compiled by the Targeted Sanctions Consortium[31].

2.3 European Union sanctions

The European Union has two objectives in using sanctions. First, the EU has acted to implement UN sanctions more effectively. Second, the EU has used sanctions as an instrument of its common policy. While international law—including decisions of the United Nations— provides legitimacy to EU sanctions, there's not a right way link to a call by the UN under Article 41 or Chapter 7 of the UN Charter in every case. In 1982 the EU Community adopted sanctions against the state in response to political developments in Poland and against Argentina following the invasion of the Falklands Islands. Subsequently, the EU adopted sanctions outside the framework of UN decisions against Belarus, China, Indonesia, Kazakhstan, Libya, Myanmar (Burma) and Zimbabwe. In cases where the EU has used sanctions outside the framework of UN decisions it's usually been to market human rights and democratization objectives in external relations. The link between sanctions and human rights has been made explicit therein sanctions are mentioned collectively instrument with which the Charter of Fundamental Rights of the eu Union (proclaimed at the great meeting in December 2000) are going to be implemented. The legal basis for EU sanctions depends on the actual measure adopted. In each case the Council, using powers conferred within the 1992 Treaty on EU (Maastricht Treaty), unanimously adopts a typical position or a joint action identifying the objectives of measures to be undertaken. From now there's divergence within the legal form. A two-stage procedure was established for economic sanctions. The 1957 Treaty Establishing the eu Community (Treaty of Rome) provides the authority for implementing economic and financial sanctions through common institutions. Article 60 contains measures associated with the movement of capital and payments while Article 301 provides the legal basis for trade sanctions. On this basis the Commission prepares a regulation containing specific measures that give effect to the political decision. The Council adopts this regulation through a professional majority vote. The regulation, which might be

[31] Biersteker T. J., Tourinho M., Eckert S. E. (ed.), (2016), Targeted sanctions: the impacts and effectiveness of United Nations action. New York: Cambridge University Press.

modified only through a unanimous decision of the Council, becomes Community law, binding throughout the EC. the utilization of Community law within the variety of regulations whose implementation is monitored by the Commission is meant to confirm uniform application of sanctions measures. However, the employment of arms embargoes by the EU requires a unique legal basis because arms and military goods remain outside the scope of the common commercial policy. There has been a necessity to scale back the danger that uneven implementation of agreed measures will diminish the effectiveness of EU arms embargoes and maybe undermine the trust between member states. The member states have sought greater uniformity through a dialogue that has led to political agreement on how arms embargoes should be applied. When an arms embargo is applied to a specific country, the states decide at the identical time whether it should be interpreted as a 'full scope' or but full scope embargo. If the embargo is to be full scope, then it's defined as being on 'arms, munitions and military equipment'. therein case, it'll apply to all or any the products on a standard embargo list. If an embargo is a smaller amount than full scope, it'll be defined as 'an embargo on arms and munitions' and therefore the member states then specify within the common list the categories that it'll cover. Additionally, the EU contains a different legal basis for travel and diplomatic sanctions since these also rest on measures that are still within the competence of member states instead of Community institutions. Travel sanctions have included bans on entry visas for specified individuals (usually senior political and military officials) and therefore the suspension of high-level visits by officials. Diplomatic sanctions have included the expulsion of diplomatic and military personnel attached to the diplomatic representations in member states and, conversely, the withdrawal of personnel attached to diplomatic representations of member states within the target country. Looking at the differences among EU and UN, the ecu Union has elaborated its approach to the employment of sanctions as a part of its Common Foreign and Security Policy, mainly in response to specific events instead of through a more 'top–down' approach. The member states have increasingly used the EU to convey effective expression to decisions of the world organization. However, the EU has also developed a particular approach to the employment of sanctions in policy areas where the UN has not provided direction, notably to support the parts of the CFSP (The Common Foreign and Security Policy) geared toward improving human rights. A recommendation by the Commission in 2001 that the EU should think in an exceedingly broader manner about how sanctions should be decided and implemented may result in further development during this area[32].

2.3.1 The decision-making process

The imposition of sanctions falls under the CFSP domain and therefore the process is regulated by Articles 30 and 31 of the TEU (Treaty on European Union). the proper to undertake initiatives lies with any member state

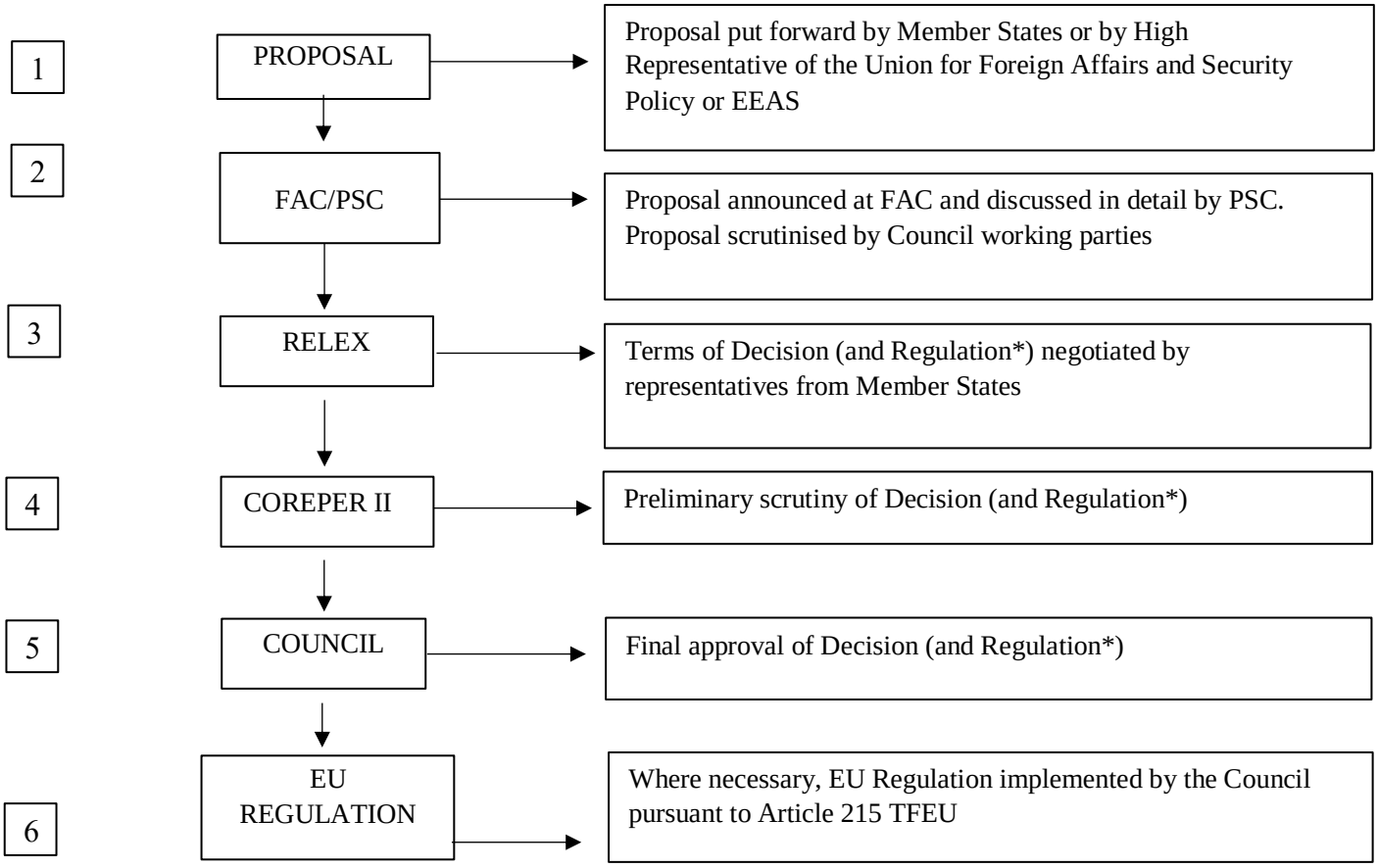
[32] Anthony, I. (2002). Sanctions applied by the European Union and the United Nations. *SIPRI YEARBOOK*, 203-230.

and with the High Representative of the Union for Foreign Affairs and Security Policy, who can act also with the support of the EU Commission.

The sanction proposal, which is commonly normally announced terms at the Foreign Affairs Council, is discussed in greater detail by the PSC (Policy and Security Committee) and scrutinised by the competent geographical working groups of the Council where member states delegates negotiate and judge by consensus who is to be listed and on the idea of what statement of reasons. The last step before the approval through the Committee of Permanent Representatives II (COREPER II) and therefore the Council is that the Foreign Relations Counsellors working party (RELEX) where the representatives of EU member states negotiate the particular and concrete terms of every and each restrictive measure. the ecu External Action Service (EEAS) enters the image very too soon altogether these procedures by making suggestions about what measures are advisable, whom to focus on with sanctions and presenting drafts of the new legal base to be negotiated well in RELEX. The Council is that the pivotal actor because it is that the forum where decisions are made, whether or not the enforcement of economic and financial sanctions required the direct involvement of the Commission when sanctions affected the functioning of the inner market. However, the Lisbon Treaty has accentuated the role of the Council which is now absorbing the implementing power that want to be exercised by the Commission; after all, the Commission can only suggest a draft of implementing regulation that in its view would make sure the common implementation of the new measures throughout the Union, but it's within the end the Council that decides and approves the regulation. There are differing kinds of targeted sanctions that fall within the previous first and second pillars as described within the Treaty of the Functioning of the European Union (TFEU). When the Council makes a choice concerning CFSP under Chapter 2, Title V of TEU, both trade and financial sanctions require a Council regulation consistent with Article 215 of TFEU (financial and economic relations) to be implemented. Under this procedure the Parliament should only learn about the choice, but Article 75 of TFEU establishes an exception. When the EU acts to forestall and combat terrorism and related activities, the Council and therefore the Parliament should adopt a regulation via the normal legislative procedure. Sanctions that comprise the previous second pillar, namely travel bans and arms embargoes, don't need further legislation from the EU beyond the Council's decision (mostly common positions before the Treaty of Lisbon, Council decisions since December 2009) with the exception of lists of specific items under arms embargoes, like dual-use items, that may be compiled by the Council in unexpected regulations. Arms embargoes are an exceptional case due to a provision on national security that has been a part of the Treaties since 1957 [TFEU, Article 346]. as an example, the Common Rules on Arms Exports approved by the Council in 2008 strictly regulate under which terms weapons is sold [Common Rules Governing Control of Exports of Military Technology and Equipment, 2008/944/ CFSP] but the ultimate word on interpreting and selecting each sale rests with national governments. The movement of individuals from and to EU countries is after all controlled by the national

governments, accountable for monitoring their borders and ensuring that the choices of the Council of Ministers are duly implemented[33].

Table 2.4 – Procedure for approval and implementation of sanctions-related CFSP decision



* Note that Regulation may not be required in addition to the Decision, but where it is, it will be proposed and negotiated in parallel with the Decision.

Table of own production; Source: Gordon R. J. F., Smyth M., Cornell T., (ed.), (2019), *Sanctions law*. Oxford, UK; Portland, Oregon: Hart Publishing.

2.3.2 The role of Common Foreign and Security Policy (CFSP) in imposing sanctions

Sanctions imposed under the Common Foreign and Security Policy (CFSP) are the EU's sanctions par excellence. While the legal documents through which they're imposed talk to them as 'restrictive measures', and also the official discourse tends to avoid the term, they're the sole measures that the label

[33] Giumelli F. (2013), "How EU sanctions work: a new narrative", in *Chaillot Papers (Paris)*, 129, May 2013, pp. 1-49.

'sanctions' is admitted. before the creation of the CFSP under the Treaty of Maastricht, sanctions were normally announced in Presidency Statements or Council Conclusions. However, sanctions regimes adopted by the EU before the conclusion of the Maastricht Treaty which remained in situ after 1993 were formalized in CFSP Common Positions. for example, the arms embargo originally imposed on Sudan in 1994 was the article of two consecutive Common Positions in 2004 before the Darfur crisis. the sole purpose of those documents was to consolidate measures associated with the sanctions regime during a single instrument, specifying the scope of the embargo and providing for exemptions. the sole exception to the rule of reformulation and consolidation of sanctions regimes during a single document is that the case of the arms embargo on China, whose informal legal basis was never transformed during a Common Position. If anything characterizes the group of sanctions gathered under this heading, it's their diversity. the kinds of sanctions contemplated within the context of the CFSP are the following: arms embargoes; visa bans; financial sanctions; flight ban; embargoes on specific commodities; diplomatic, cultural and sports sanctions. The arms embargoes are the most frequent type of EU sanction. Arms embargoes typically forbid the 'supply or sale of arms and related material of all kinds including weapons and ammunition, military vehicles and equipment paramilitary equipment, and spare parts of the aforementioned. The imposing instruments exempt the supply of 'equipment intended solely for humanitarian or protective use'. Financial sanctions comprises a large style of measures. the foremost frequently applied financial sanctions is that the freezing of assets of people included in blacklists. Regarding the flight ban, the legal difficulties encountered within the episode of Yugoslavia in 1998 appear to possess made the employment of this measure undesirable and sporadic. Nevertheless, after the forced and illegal landing of a flight in Minsk last May, the eu Union imposed various sanctions on Belarus (this case are going to be analysed in additional detail within the following section), including a flight ban. Embargo on specific commodities is taken into account a targeted sanction because it applies on a product of special importance for the continuation of the activities of the party judged to be guilty. Eventually, diplomatic, cultural and sports sanctions could be a heterogeneous group encompasses measures like the limitation of contacts, the invitation of political dissidents to national celebrations at embassies abroad, the suspension of scientific cooperation or bans on participation in international cricket tournaments. The scarce attention received by such measures in discussion on targeted sanctions is because of their low profile[34].

[34] Portela, C. (2012). *European Union sanctions and foreign policy: when and why do they work?*. Routledge.

2.3.3 Case Study: European Union v. Belarus

Belarus' relations with the international community and, especially, with its larger western neighbour – the eu Union (EU) – have shown little sign of change since the mid-1990s, and at the best may well be described as a spasmodic: for each intention to cooperate, there always seems to be a counteraction to thwart it. as an example, an initially enthusiastic ratification of Belarus 'Partnership and Cooperation Agreement (PCA) with the EU in 1995 resulted in suspension only two years later, attributable to its declining human rights record. A subsequent rapprochement in 1999 – as a part of the "Responsible Neighbourhood" strategy – instead concluded within the signing of a Union Treaty with Russia. Efforts for more dialogue under the eu Neighbourhood Policy (ENP) in 2004 and a subsequent Eastern Partnership Initiative (EaP) in 2009, yielded only partial involvement of Belarus, in an exceedingly non-binding multilateral track of regional cooperation. A Joint Interim Plan carrying substantial financial incentive, but straightjacketed by political conditionality, disintegrated after the 2010 presidential election. The 2012 Dialogue on Modernization, targeting civil society, to date, as claimed, has had only a limited effect. a way of impasse around EU-Belarus relations has now grown into a way of fatigue amongst policymakers, donors, and even practitioners, leading to half-measures normally wanting action and commitment. Donors are particularly wary of Belarus-focused discussions, and presently there seems to be a tacit acceptance of the established establishment. Meanwhile, Belarus' relations with its eastern neighbours have predictably expanded, albeit more often through compulsion, instead of by discretion. By 2007 Belarus was co-opted into negotiation over the Eurasian union (ECU) with Russia and Kazakhstan, which took force in 2010. By May 2014 the ECU member-states signalled a joint agreement on the possible launch of the Eurasian Economic Union (EEU), to return into effect in January 2015. So, because it seems, Belarus' domestic and peacekeeping remain emphatically stagnant, reflecting a predictable established order, or do they? Two critical disjunctures challenge a seemingly enduring order. the primary disjuncture refers to the government's quiet but persistent discourse of resistance to Russia's overbearing influence, manifested in three long years of sabotaging the launch of the ECU and petty wars over trade and economic issues; in re-shaping the Eurasian course into a cumulative integration narrative to remain connected with both the East and also the West; in an exceedingly recently increasing dialogue with the EU; and more tellingly, in publicly endorsing Petro Poroshenko's leadership in Ukraine and objecting to Russia's demands for extending an economic and political embargo to the country. The second disjuncture is far and away more emblematic of existing undercurrents at work, exposing profound longitudinal changes in public opinion and behavior related to growing levels of affinity and interest within the EU, moreover because the public's gradual legitimation of European standards and fostering of a brand-new European identity – "We are a part of Europe", a narrative hitherto absent from a public "story-telling". this means an ongoing process of socialization into a eu discourse and a wider European space, manifested at different levels and by different actors. In turn, this might also suggest that the EU, despite a

limited official dialogue, might need been doing something "right", to be ready to achieve expanding the boundaries of public space and even engendering a replacement sense of identity. This triggers a spread of questions, with three perhaps being of particular relevance: (1) what has been the EU's strategy thus far, especially within the circumstances of no political dialogue; (2) how does this translate into public/government narratives; and (3) essentially, if there are changes, why now and what of democracy?[35] There are several issues that divide Belarus and therefore the global organization politically. These issues relate primarily to the restriction of democratic procedures and violation of human rights, and to the border control. Belarus is that the just one European state that also remains the execution as its law. The Human Rights Watch stated within the annual (2016) report (www.hrw.org), that "the capital punishment remains in use. Officials pressure and arrest human rights activists and critics on spurious charges. Authorities regularly harass independent and opposition journalists. Legislative amendments further restricted freedom of expression, specifically Internet freedom". the eu Union put a problem of corporal punishment ban as important condition for the development of its relationship with Belarus. In 2015 Belarus expressed its readiness to debate this issue with the Council of Europe, however, executing remains in function. A second issue relates to the arrests and harassment of human rights defenders and government critics. Belarusian authorities interfere with the work of independent and opposition journalists and bloggers. enforcement officials intensified prosecutions of independent freelance journalists for cooperation with unregistered foreign media. there have been several cases against journalists, in step with the Belarusian Association of Journalists. All cases resulted in significant fines for the journalists. Freedom of association is additionally violated in several aspects. Thus, the authorities still enforce legislation criminalizing involvement in an unregistered organization, and at the identical time arbitrarily deny registration to and try to dissolve nongovernmental organizations (NGOs). At the identical time, Belarusian authorities perceived to be seeking a political rapprochement with European governments and institutions, and hosted variety of high-level visits. this implies that Belarusian government started new steps toward the ecu Union wishing to boost the link. Among the discussed issues are migration, regional conflicts, border control, etc. The 2004-2007 EU enlargements have brought Armenia, Azerbaijan, Georgia, and particularly Belarus, Moldova, and Ukraine closer to the EU borders. Therefore, problems with bilateral security and stability became more important, and therefore the special program was designed aimed to resolve this issue. The EU started the European Neighborhood Policy in 2004 and developed different means to succeed in out and to shape the surface by its own standards. This included several financial and policy instruments that specialize in different aspects of regional development in Eastern Europe. a number of them were more popular, some failed soon. Program of Eastern Partnership (EPP) was established in 2008. A joint declaration was signed in Prague in 2009. It included 6 ex-soviet states: Belarus, Moldova,

[35] Korosteleva, E. A. (2016). The European Union and Belarus: democracy promotion by technocratic means?. *Democratization*, Volume 23, Issue 4, 678-698.

and Ukraine that have borders with the EU, and Armenia, Georgia and Azerbaijan within the Asian region. Eastern partnership program proposes ideas for enhancing the EU's relationship with the region, including within the field of home affairs. In the future these six countries were viewed as friendly allies to the EU. Therefore, Program of Eastern Partnership had two sides: political and economic, and economic funds rely on political steps made by any of the ex-soviet republics toward the EU requirements. This program was successful for the EU in many aspects: soon the so called "colored revolutions" befell in Ukraine and Moldova that led to radical changes in their policy and attitude to Russia. Georgia got eliminate Russian influence even before joining Eastern Partnership Program. Therefore, in 2014 the EU signed the Association Agreements with Georgia, Moldova and Ukraine, and also the European Parliament passed a resolution recognizing the "European perspective" of those three post-soviet countries. In 2017 the EU opened the border for Ukrainians (cancelled visas) and promised to debate the problem of Ukrainian inclusion into the EU within the future (however, in keeping with the Eastern Partnership strategy, the EU is unlikely to just accept these states within the near years, this can be a future perspective for them). things with Belarus differs greatly. Eastern Partnership Program failed to meet Lukashenko's expectations, it absolutely was poorly funded for Belarus: practically, European money went only to the projects on strengthening the border control and to not the economic development of Belarus. No political benefits were provided for Belarus likewise (for example, visa cost for Belarus is 60 euro, while for other countries within the region it's 30 Euro or free). Negative evaluation of presidential campaigns (2006, 2010) in addition as sanctions didn't positively influence the connection with the EU. Therefore, although Belarus joint the Eastern Partnership program, this program wasn't actively supported by Lukashenko. He didn't change political priorities of Belarus and failed to make a turn from Russia to the EU, just like the above-mentioned three republics in Eastern Partnership Program. On the contrary, Lukashenko increased security for his regime and prevented any opposition attempts to start out the "color revolution" in Belarus. However, the EU political goals in EPP didn't take into consideration the interests of eastern European countries and understand them as equal partners: the "othering" or differentiation of Eastern European countries was interpreted as deviation if they failed to accept the EU values and norms. National priorities of Belarus as expressed by President Lukashenko (including its close relationship with Russia) have not been accepted by the EU. within the official EU-Belarus talks until recently (i.e., the Russia-Ukraine deterioration of relations in 2014) Belarus normally was treated as a "a bad guy" who still had to produce security on the EU borders and accept the EU interests[36]. The historical and political context described above has obviously also influenced the sanctions that are imposed on Belarus over the years. The sequence of sanctions starts with the measures imposed within the wake of the enactment of a brand-new constitution concentrating powers on President Aleksander Lukaschenko in 1996. In response, the

[36] Titarenko, L. (2018). Belarus and the European Union. From confrontation to the dialogue. *CSE Working Papers 18| 01: febbraio 2018*.

Council took variety of measures: it withdrew support from Belarus' application for membership of the Council of Europe, ceased high-level contacts and technical assistance programmes, froze the ratification of the already concluded PCA – a gesture matched by the ecu Parliament's announcement that it might not assent to any bilateral agreement with Belarus. These measures were 'informal' as they weren't adopted during a legally binding CFSP document. a number of these sanctions were temporarily lifted following the establishment of an Advisory Monitoring Group (AMG) in Minsk in 1998, a platform for dialogue between the authorities and therefore the opposition, under the umbrella of the Organisation for Security and Co-operation in Europe (OSCE); nevertheless, measures were re-imposed after the Belarusian authorities withdrew their authorisation in 2002[37]. In more recent times, Belarus has started a replacement wave of post-soviet transition. Still being nationalistic and paternalistic, the country is becoming more receptive the West and making development towards the European Union. For this reason, in 2015 most of the Western political and economic sanctions were suspended, and therefore the relationship between the European Union and Belarus got improved. In fact, relations between the European Union and Belarus have deteriorated further over the past two years. After the elections of 9 August 2020, won by Lukashenko, the EU adopted numerous sanctions, starting in October of that year. The first package of sanctions was adopted in response to the fraudulent nature of the August 2020 presidential elections in Belarus and therefore the intimidation and violent repression of peaceful protesters, opposition members and journalists. The EU doesn't recognise the results of the elections in Belarus, which it condemns as neither free nor fair. These first restrictive measures include a travel ban and an asset freeze against 44 persons identified as being answerable for the repression and intimidation of peaceful demonstrators, members of the opposition and journalists within the aftermath of the 2020 presidential elections in Belarus, similarly as irregularities within the electoral process. Subsequently, a second round of sanctions was imposed on President Alexander Lukashenko and 14 other officials, including his son and national security adviser Viktor Lukashenko. Again, this involves a travel ban and asset freeze. EU citizens and firms are prohibited from making funds available to listed persons. Similar sanctions have followed against high-ranking officials and business leaders who support the Lukashenko regime. In 2021, following the airplane landing of a Ryanair flight in Minsk on 23 May, the Council decided to impose restrictive measures against 78 individuals and eight Belarusian entities. the choice was taken seeable of the escalation of great human rights violations in Belarus and also the violent crackdown on civil society, the democratic opposition and journalists. Additionally, seven persons and one entity subject to the current new round of restrictive measures were designated in reference to the forced and illegal landing of a Ryanair flight in Minsk, Belarus, on 23 May 2021. The Council selected 4 June to bolster the present restrictive measures visible of true in Belarus by introducing a ban on overflights of EU airspace and

[37] Portela, C. (2011). "The European Union and Belarus: Sanctions and Partnership?", *Comparative European Politics,* Volume 9, Issue 4, 486-505.

access to EU airports by Belarusian carriers of every type. At the identical time, the European Union concerned the discharge of journalist Raman Pratasevich and his companion Sofia Sapega. The aim of those sanctions is to place pressure on the Belarusian political leadership to interact in a very genuine and inclusive national dialogue with society at large and to avoid further repression. The EU stands able to support a peaceful democratic transition with a spread of instruments, including a comprehensive plan of economic support for a democratic Belarus. it's also able to take further measures, including against other economic actors, should matters in Belarus does not improve[38]. Eventually, over the time, sanctions ultimately proved successful due to the leadership's desire to preserve wealth. Nevertheless, it absolutely was the not primarily CFSP sanctions that worked, but the absence of a PCA, of links of cooperation and assistance, and in an exceedingly nutshell, of integration into a multilateral setting, which made the country attractive for investment. The Belarusian leadership softened its stance when it realized it absolutely was not able to cope within the absence of increased Western investment. Thus, the promise of cooperation and its by-products – enhanced trade, foreign investment and assistance – worked better as a persuasion tool than CFSP blacklists. Progress towards a limited rapprochement was only made possible by the character of targeted sanctions[39]. On the opposite hand, the method towards a peaceful and democratic transition in Belarus appears slow and complex, intertwined with numerous issues that are difficult to manage and that a tightening of sanctions or a replacement package doesn't always seem to satisfy the objectives that they're imposed.

2.4 The geopolitical meaning of energy sanctions

As discussed above, it's rather complicated to answer the question "are sanctions effective?". The analysis of the sanctioning instrument can't be separated from the context during which they're imposed. The role of the international organisations (above all the UN and also the EU) and of the States has changed over time precisely to deal with the various contexts and therefore the different political situations that follow each other in implementing sanctions against different entities and/or subjects. However, what we are able to say with certainty is that sanctions have a powerful link and robust consequences with geopolitics. the 2 fields are intertwined both when sanctions are implemented and once they get or end. The evolution of the sanctions instrument, with the passage from Comprehensive to Targeted Sanctions, provides a clearer picture within

[38] European Union (2021), "Restrictive measures following the 2020 Belarus presidential elections", *Sanctions: how and when the EU adopts restrictive measures*, Internet: https://www.consilium.europa.eu/it/policies/sanctions/restrictive-measures-following-the-2020-belarus-presidential-elections/ (viewed on 21/08/2021).

[39] Portela, C. (2011). "The European Union and Belarus: Sanctions and Partnership?", *Comparative European Politics,* Volume 9, Issue 4, 486-505.

the reading of this close relationship. As is well-known, the impact of a sanctions package is multidirectional, the greater the sanctions, the greater the number of sectors affected, and this could cause a tightening of bilateral relations at the geopolitical level or a rapprochement, looking on the response following the reception of sanctions by the State and/or the targeted entities. Among other areas, I've got chosen to explore the link between geopolitics and energy. The latter has become increasingly important over the years, especially as a tool that may act as a actuation for a country's economy, especially in developing countries. Just as energy abundance isn't a path to selective isolationism, we want to assess whether, when and the way such abundance might justify using energy as an instrument of national security. the employment of energy as a tool to influence neighbors and hurt enemies isn't new or unique to the us. One can argue whether such a precept is moral. If the alternatives are war, are otherwise ineffectual, or leave violations of law of nations unchecked, then energy policy should be accustomed protect national security interests. There have certainly been cases during which energy suppliers have used market dominance to coerce political and economic concessions from their neighbors. Right or wrong, it'll happen again. presumably, nations will decide whether to wield energy as a national security tool supported their perceptions of whether doing so will succeed. Countries that attempt to use energy as a geopolitical weapon should understand their chances to supply the required outcomes. Countries that are subjected to such tactics will inevitably try and circumvent the impacts. No analytic model can predict every outcome from political interventions in energy markets, but a systemic approach to understanding the potential risks and impacts may produce better outcomes. Ideally, decisions to intervene in markets would be designed, misguided or unrealistic policies wouldn't be implemented, and dangerous interventions would be more easily countered. This work proposes a brand-new analytic framework called the principles of Six. The foundations of Six aren't prescriptive. They hinge upon six tactical interventions that capture most tools nations could use as an instrument of national security policy to intervene in energy markets. The Rules propose that any given intervention must be assessed against six market and institutional factors that may influence the specified outcome. No individual factor may signal success or failure. Taken together, these factors will inform whether a proposed intervention are able to do the size and longevity, mobilize the market players, and convey the political and policy clarity necessary to attain the intended impacts. Further, we should always assume that countries tormented by any intervention will use such a technique to counter interventions against them. If accustomed test either side of a market intervention and therefore the geopolitical impacts, the foundations of Six provide a foundation for a cyclical approach to assess policy outcomes over time and whether or not they may be sustained. The six market interventions are tactical options that may influence energy markets to serve national security interests. the primary five tactics reflect the history of energy trade over the past century. The last tactic reflects the emergence of global climate change as an overseas policy issue and therefore the imperative to grasp whether national and global climate policies will influence investment choices to extend the competitiveness of fresh and renewable energy and energy efficiency.

• Block Exports: most frequently, interventions to dam exports manifest themselves as sanctions on a country's exports so as to deny that country markets and revenue. US and European sanctions on Iranian oil exports are, perhaps, the foremost prominent recent example.

• Constrain Production Capacity: Production from some countries is so large that blocking production would be hugely complicated, or curtailing production could raise global or regional prices and inflict equal or more pain on those imposing the sanctions. Instead, this intervention would block investment and trade, thereby affecting the long run growth of the energy industry, as this might affect interest rates and also the ability to finance budget deficits and company debt. This approach underpins current US and European sanctions on Russia.

• Flood Markets: A producer country, or countries, might use their capacity to flood markets so as to drive out new competitors, acquire market share, or punish others with a high stake in expanding market share. If energy producing countries rely on an oil reference price to balance budgets, driving down the worth of oil could have far-reaching impacts. Anti-dumping regulations were developed by the planet Trade Organization to forestall such tactics in most commodity trade, but oil and gas trade aren't included.

• Starve Markets: Dominant suppliers may attempt to use access to provide as how to govern highly dependent customers with few options. Russia has such a dominant relationship over Ukraine, Bulgaria, the Baltic states, and Finland. If a rustic takes such an approach, it can jeopardize its international role as a stable supplier. The Arab Oil Embargo in 1973 led consumers to counter the danger of market disruptions with the creation of the International Energy Agency. A comparable case would be to interdict supplies to a market, as occurred with Japan during war II.

• Assist Friends: Targeted energy supplies or technical support to develop energy resources could help friends survive an emergency, build capacity for the longer term, and forestall others from taking advantage of transitional weaknesses. This was the rationale behind Congressional calls in 2014 to expand US LNG exports to Ukraine after the Russian invasion, although exporting companies couldn't physically accelerate deliveries beyond contracted schedules. Another example has been Venezuela's use of Petrocaribe to subsidize fuel and win the allegiance of Caribbean nations.

• Change the Fuel Mix: Countries might use financial, technical, and diplomatic tools to induce other nations to change their fuel mix and make it more sustainable. Unless cleaner kinds of energy production end in comparable rates of return as coal—which means lowering the price or intermittency of renewables, pricing coal externalities, or both—then the long run trend in China, India and geographic region are to expand coal generation, in many cases more quickly than renewables. temperature change negotiations may lead to targets to cut back gas emissions. The impact of these targets must be assessed against market incentives which will drive capital flows and investment choices. The above tactics might succeed or

fail supported six prevailing market factors, how countries incorporate these factors into their interventions, and the way targeted countries use their knowledge and influence over their own markets to respond:

• Market Scale: Big interventions are always harder and riskier. The larger a producer's contribution to global or regional markets, the harder it'll be to dam its exports (e.g., Iran v. Russia in scale). The larger the buyer, the harder to starve the market. The smaller the region or country, the simpler to support friends or influence investments that affect the fuel mix. The larger the economy, the harder to pivot on switching fuel choices.

• Investment Flows: Constraining a nation's production and exports of fuel requires curtailing investment flows into energy development. As long as there are contributions to production potential, increased productive capacity will find its thanks to market. Conversely, assisting allies will fail if they're not also aligned with investments which will change an underlying dependence on a selected supplier. Investment flows will fundamentally determine national energy infrastructure and climate impacts.

• Coalitions: Actions to intervene in markets will create market opportunities to counter them. Coalitions with key public and personal actors usually are going to be necessary to confirm that tactics to influence supply or capital flows aren't simply circumvented. Countries have to collaborate in order that sanctions on one country don't become another country's vehicle for increased competitiveness. Additionally, to national cooperation, banks and financial institutions must be willing to cooperate. altogether tactical areas, coalitions can accelerate desired outcomes, and also the failure to keep up them can undermine the specified intent.

• Ability to Sustain: If there's a market intervention, countries must have the flexibility to sustain it for sufficient time so as to own a reputable impact. Interventions seen as short-term will cause speculation about their ability to own an enduring, strategic impact. Speculators will sweep in to achieve from large supply injections. Meager support for friends might be counterproductive if the sole longterm supply source could be a predatory supplier.

• Speed: Alacrity in performing on stated goals is essential to demonstrating seriousness of purpose. as an example, President Vladimir Putin's judgment of a delayed and tepid response from the us and Europe to inflict pain after annexing Crimea may have encouraged even further incursions into Ukraine. Interventions are only when targeted countries haven't had time to arrange against them. On fuel investment issues, delay in incentivizing cleaner options may entrench carbon-intensive infrastructure alternatives.

• Self-Risk: Governments will assess possible sanctions and other interventions in energy markets vis-à-vis impact on national businesses. Immediately after Russia invaded Crimea, for instance, Europe and therefore the us may have given greater weight to the impact of sanctions on their respective national companies than to the strategic significance of Russia's violation of Ukraine's sovereignty and territorial integrity. Nations must consider how interventions balance national security and commercial objectives then assess whether the

proposed tactics will achieve the required impacts, not just whether those tactics remain domestically palatable. European and American sanctions against Iran were intended to pressure Iran into negotiations to preclude it from gaining a WMD. The sanctions imposed in January 2012 denied entities importing petroleum from Iran access to European and American financial markets. Blocking imports from Iran was considered viable because Iran's share in global markets was relatively small: about 2.5 million barrels per day (b/d) in exports in 2011 relative to a market of about 89 million b/d. These sanctions could have failed when oil prices shot up to $125/barrel in February– March 2012 and purchasers of Iranian oil all sought new suppliers in a very short timeframe. Active discussions started within the us and Europe and with the International Energy Agency to think about releases of strategic petroleum reserves. Oil prices began to fall in June 2012 as Asian country versed market demand, and as US production—for completely unrelated reasons—added 1 million b/d to global supplies that year. in this context, the us convinced importers of Iranian oil to contemplate how overreliance on Iran could make them vulnerable. The us invited these countries to diversify their supply. Every major importer of Iranian oil responded by cutting oil imports from Iran by 15–20 percent. India, as an example, agreed to scale back its imports after a State Department team met with each Indian refinery that imported Iranian crude and reviewed its options for diversification. China made a national security decision to review the structure of its oil imports and further diversify supply. Turkey determined that sanctions would exclude its sole importer of Iranian crude from US financial markets and would entail greater costs than purchasing oil from other sources. At its peak, this coalition took 1.4 million b/d of Iranian oil off international markets. The combination of sanctions and also the subsequent oil price collapse in 2014/2015 denied Iran on the dimensions of $5.7 billion a month, almost inevitably contributing to Iran's willingness to conclude on July 14, 2015 an agreement with the five permanent member of the UN Security Council plus Germany (known because the P5+1) to contain its nuclear program reciprocally for sanctions relief. With oil prices roughly at $100 per barrel at the beginning of 2012 and Iranian oil exports at about 2.4 million barrels per day, Iran's oil revenue from exports was about $7.2 billion per month. The loss of 1.4 million b/d in exports alone accounted for a $4.2 billion loss in monthly revenue. With Brent oil prices falling from about $100 in 2012 to about $50 per barrel within the half-moon of 2015, Iran lost another $1.5 billion in monthly revenue. The IMF estimates that Iran needs $122 per barrel to balance its budget. For Iran, it became imperative to return to international oil and capital markets. By 2015, US and European sanctions and international market developments had created the financial leverage that helped change the Joint Comprehensive Plan of Action, intended to scale back Iran's enriched uranium and centrifuges, redesign the deuterium oxide reactor at Arak, afford intrusive nuclear inspections, account for possible military dimensions of previous Iranian activities, and eventually afford sanctions relief. By the time this paper is published it should be clear if the US Congress rejects or approves the JCPOA, and if it's rejected, whether President Obama can sustain a veto. Many Republicans within the legislature and a few Democrats have objected to several elements of the JCPOA, particularly because it still allows Iran to take care of some sort of military program. Some argue that

tougher sanctions should be imposed so as to hunt greater concessions. the principles of Six would suggest that the sanctions regime may have already reached its peak of influence, which the P5+1 indeed concluded the JCPOA when their leverage was highest. With Iran having agreed on a global deal to limit its nuclear program, the moral authority to sustain support from China and Russia fades rapidly if the us rejects the JCPOA. China, furthermore, has little to lose. China has isolated one trading company and one bank to handle commercial and financial transactions with Iran, and both are already under US sanctions. the eu Union and therefore the UN council have also endorsed the JCPOA, suggesting that they'd have little basis to enforce tighter sanctions. Iran, for its part, desperately needs oil revenues, and one should expect them to supply discounts to secure even limited revenue flows. China would be the primary country to profit by drawing on discounted oil to make its international reserves. If the US rejects the JCPOA and seeks a tighter sanctions regime, it should expect to act alone, without the advantage of the coalition that made the 2012-2014 round of Iran sanctions succeed[40].

2.4.1 Case study: US v. Iran

Iran is no stranger to sanctions. The US imposed its first sanctions on the country after a gaggle of radical students seized the American embassy in Tehran almost four decades ago; the Iran hostage crisis has been seared into American public memory and policy toward Iran. The United States has widened the scope of those sanctions since then, with substantial expansion under the Trump administration. The sanctions against Iran broadly apply to science (including nuclear research), military, and most significantly trade (including oil, Iran's largest export). But in spite of those measures to isolate Iran—and oil exports hitting record lows in 2019—it continues to be one amongst the ten largest oil exporters within the world. Iran has seen such (still limited) economic success even within the face of strong US sanctions because, unlike within the case of Democratic People's Republic of Korea, a number of the world's largest economies have used a spread of innovative strategies to bypass unilateral US sanctions on Iran. This literature review will critically examine the dialogue on and implementation of those strategies to raised understand how and why countries navigate trade with a sanctioned nation. When the United States imposes sanctions on a rustic, there's traditionally an expectation that allies and trading partners will follow. Conducting business with a US-sanctioned country is comparable to "shooting yourself within the foot," as no American company will trade with you or your financial institutions. Yet even facing the pressure of the US and plenty of its allies, the Iranian government has still did not satisfy policymakers within the Trump administration. On June 24, 2019, President Trump placed additional sanctions on Iran. On January 8, 2020, in retaliation to the US-drone killing of Major General Soleimani, Iran launched ballistic missiles against US bases in western Iraq. That attack was met by even more

[40] Pascual, C. (2015). The new geopolitics of energy. *The Center on Global Energy Policy. Columbia University in the City of New York School of International and Public Affairs (SIPA)*.

US sanctions two days later. The international organisation, however, has not matched US measures. The United Nations SC (UNSC) has been sluggish in their imposition of sanctions against Iran, having last imposed sanctions in July 2015. This absence of sustained multilateral pressure on Iran has made it difficult to bring Iran to the negotiation table. Were the UNSC to require stronger action, Iran may become more constructive in its attempts to finish the worldwide sanctions regime. within the meantime, countries have adopted measures to regulate to a brand new normal of limited trade with Iran[41]. Some analysts believe that if the Trump administration is serious about shaking up U.S. policy, increasing energy security would be the primary step. one among the goals of the administration has been to renew sanctions on Iran's energy sector. this can create a chance for the U.S. energy industry to enforce "the right imposition policy." Finding new markets for U.S. LNG and oil is also facilitated by sanctions against Iran. The shale-gas boom provides the us the chance to become one in all the world's leading condensate exporters. South Korea imports about 70 percent of Iranian oil as condensate and, consistent with Iran's Ministry of Oil, Iran supplies 50 percent of South Korea's condensate. During the Obama administration, the u. s. was unable to export such amounts, but attributable to the shale boom, it can currently export condensate to Asian nation and reduce its reliance on Iran. there's a difference between oil exported from Iran and therefore the u. s. in terms of its chemical composition. Iran's export-oil grades are sourer and heavier than the sunshine, sweet crude that U.S. shale produces in record amounts. With American energy independence and even the entry of gas exporters, we'll see fierce competition among gas-export cartels, which is able to lead to lower prices and closer regional gas prices. Reducing revenues are a serious challenge for energy exporters, most of which are rentier governments. Qatar and Saudi Arabia will face budget-deficit problems. The decline of U.S. dependence on geographic area energy producers will naturally affect their domestic and foreign performance. Therefore, the requirement to implement policies like higher tax rates and more economically sound policies during this region are almost unprecedented and can likely cause public discontent. The political and domestic instability in energy-exporting countries within the geographical region can cause changes in their foreign policies and people of the US. The sanctions imposed on Iran and Venezuela have caused the heavier crude employed by U.S. refineries on the seacoast to be aloof from the market. This has resulted in a rise in price differentials. However, Pascual states that this could not be permanent, because the shipping industry needed a brand new reasonably high-sulfur sludge like fuel. Iran, with its vast oil and gas resources, has to date did not use energy exports in its policy. Although it's the second-largest gas reserves within the world, its share of the world market is a smaller amount than half a percent. Exports that expand Iran's share of the regional and global energy market would ultimately make it possible to extend both regional security and trade volume by creating interdependence. Shale oil has given confidence to U.S. administrations to drive forward

[41] Bootwala M. (2020), "The Iran Problem: An Evaluation of US Sanctions on Iran and Global Reaction", *Georgetown journal of international affairs*, Volume 21, pp. 136-141.

their foreign policies. Energy abundance has forced the us to search out customers overseas to simultaneously reduce the role of rivals like Russia and enemies like Iran in coping with emerging economies and to ensure that the oil and gas industry can continue running in an exceedingly volatile market. within the industry, approximately 55 percent of crude is sold on long-term contracts between seller and buyer. The long-term contract hedges the risks of an oversupplied marketplace for the vendor and helps buyers obtain a relentless quality of fossil oil for designated refineries. It also assures that in an exceedingly tight market, supply won't be disrupted and cause pain from shortages[42].

2.4.2 Latest development: the Joint Comprehensive Plan of Action (JCPOA) and the two new presidencies: what are the possible scenarios?

In autumn 2013, Iran appeared to be on the brink of becoming a nuclear-armed state. It had nearly 20,000 uranium-enrichment centrifuges in place and was installing them at a rate of more than 700 per month. Around 1,000 second-generation centrifuge models that were three times more effective appeared to be ready for operation, and more were being prepared for installation. Iran's stockpile of low-enriched uranium (LEU) was growing at an average rate of 150 kilograms per month, and it had almost enough 20%-enriched uranium hexafluoride for a weapon, if further enriched.

By 2013, Western powers had been negotiating with Iran for ten years, attempting to curb a nuclear programme with little economic justification and which many Western strategists saw as a stalking horse for nuclear-weapons development. When France, Germany and the United Kingdom (the E3) negotiated with Iran on their own from 2003–05, they persuaded Iran to suspend part of its uranium-enrichment programme, but they could not convince Iran to forgo enrichment altogether. The so-called 'right to enrichment' was a rigid sticking point.

From 2005–10, the United Nations adopted increasingly sharp sanctions resolutions while Iran steadily increased its enrichment capability. In what might be called a race between centrifuges and sanctions, the centrifuges were winning. Uncompromising positions on both sides meant that negotiations between Iran and the five permanent members of the Security Council plus Germany – usually called the P5+1, although referred to in Europe as the E3+3 (the E3 plus China, Russia and the United States) – and chaired by the European Union were fruitless.

In June 2013, the dynamics changed with the election of Hassan Rouhani, a pragmatist who had campaigned on a pledge to improve Iran's stagnant economy by getting sanctions lifted. It is important to note, however, that earlier that year, Ahmadinejad had authorised secret bilateral talks in Oman with emissaries from US

[42] Kalehsar O. S. (2020), "The geopolitics of U.S. energy sanctions against Iran", *Middle East policy*, Volume 27, Issue 2, pp. 108-119.

President Barack Obama. These talks also had the approval of Iran's Supreme Leader Sayyid Ali Khamenei. The agreement that was finally reached in Vienna on 14 July 2015 included more Iranian concessions than many observers had expected. It required Iran to eliminate all of its usable 20%-enriched uranium and 98% of its 3.5% LEU, and to limit LEU stockpiles to 300 kg for 15 years. Iran had to remove 14,000 of the 20,000 centrifuges installed at the Natanz plant. They would be kept in storage, giving Iran scope to restore enrichment production to previous levels in case the agreement broke down. (In practice, moving the centrifuges likely impaired their functioning.)

For 15 years, enrichment could continue only with 5,060 inefficient and breakdown-prone first-generation (IR-1) centrifuges and only up to 3.67% (the level needed to fuel most power reactors). During this same period, enrichment would cease at Fordow, although the plant could remain open with 1,044 centrifuges in a non-enrichment function to produce stable isotopes. The calandria (core) of the Arak reactor was to be removed and disabled, and the reactor redesigned, so as to minimise its ability to produce weapons-grade plutonium. Iran agreed not to engage in spent-fuel reprocessing for 15 years. Enrichment-related research and development was limited for eight years, after which it could gradually expand at an agreed schedule, as set out in Annex I to the deal. Iran was not to construct additional heavy-water reactors or accumulate heavy water for 15 years; all excess heavy water was to be made available for export to the international market. Iran was restricted to stockpiling no more than 130 metric tonnes of heavy water ahead of the redesign of the Arak reactor.

False accusations of Iranian violations served to validate Trump's claims before and after his election that the JCPOA was the 'worst deal ever'. It took 16 months, however, before he took decisive action to withdraw from the agreement. The president of the United States has the authority at any time to issue an executive order applying new sanctions or reapplying old ones that were eased under the JCPOA. Trump could not unilaterally carry out his election pledge to 'rip up' the multilateral agreement if the other seven parties wanted to preserve it, but he could end the waivers of US sanctions that provided the largest trade-off for the compromises Iran was making.

Meanwhile, diplomats from Western parties to the JCPOA had been working intently with their counterparts in the State Department to address Trump's demands. They came very close to consensus on a package that would complement the JCPOA. The allies would confirm the right of the IAEA to conduct inspections anywhere it has reason to believe nuclear activity might be taking place, and they would declare that any Iranian long-range missile development would trigger strong pushback. Trump's demand to abolish the JCPOA's sunset provisions on nuclear enrichment were the most difficult issue, because imposing permanent restrictions on Iran's enrichment capacity was an obvious deal breaker for Iran. France, Germany and the United Kingdom knew that Iran would not accept unprecedented and perpetual limits. The diplomats came up with a way, however, to have the limits extended on a voluntary basis. They would declare that if Iran's future nuclear capabilities were not proportional to its civilian energy programme, they would reserve

the right to reimpose sanctions. Given that Russia had agreed to supply fuel for the reactors it provides, Iran would not need an industrial-sized enrichment programme for the foreseeable future, they judged. A fourth pillar of the supplemental agreement among the allies would address Iran's regional military activity in Syria and Yemen by sanctioning Iranian militias and commanders intervening in either country or involved in missile transfers. Efforts to meet Trump halfway were fruitless. Calling it 'insane' to oppose agreements recently entered into, Macron said at the end of his trip that Trump was set to pull out of the deal as part of 'a strategy of increasing tension' and for domestic political reasons. Trump's hawkish new security team reinforced his political inclinations. On 9 April, former ambassador to the UN John Bolton took over as National Security Advisor, replacing McMaster. Bolton had been a long-time advocate for regime change in Iran, which he has called the 'only long-term solution' to the threats posed by the country, and for the termination of the JCPOA, rather than trying to improve it. Long before Trump's election, in the final months of negotiations on the JCPOA, Bolton advocated military action as the only way to stop Iran's nuclear programme. Pompeo, too, had previously argued for regime change in Iran: as a member of the House of Representatives, Pompeo had called upon Congress to 'change Iranian behavior, and ultimately, the Iranian regime'. Trump's withdrawal immediately isolated the US. Apart from four states in the Middle East – Bahrain, Israel, Saudi Arabia and the United Arab Emirates – the reaction was alarm and despair. Europeans, in particular, were dismayed over the assault on one of the EU's greatest foreign-policy achievements and the secondary sanctions that Trump threat-ened to impose on their firms doing lawful business with Iran. Pouring salt in the wound, US Ambassador to Germany Richard Grenell in his first day on the job on 8 May doubled down on US demands, tweeting that 'German companies doing business in Iran should wind down operations immediately'. European Council President Donald Tusk summed up the mood when he condemned the 'capricious assertiveness of the American administration', and tweeted: 'with friends like that who needs enemies'. The transatlantic rift looked to be at its widest in decades.

The JCPOA was far from perfect, and the unsettled issue of Iran's past nuclear-weapons development left an indelible blemish. It involved compromises, like any negotiated agreement. Before the US withdrawal, however, it was running smoothly. Iran was honouring its commitments and minor issues were being resolved. If left in place, JCPOA implementation could be further improved in ways that do not require renegotiation of the deal itself. The Joint Commission established under the JCPOA to address complaints and ambiguities has had success in deciding on technical issues that were left undefined, such as the number of advanced centrifuges Iran is allowed to operate for research and development purposes.

It should be clear that more sanctions will not cause Iran to buckle under and renegotiate the JCPOA on US terms, especially when no other major partner voluntarily supports new penalties. Sanctions helped bring Iran to the negotiating table, but they are not what persuaded it to cut back its nuclear infrastructure and accept intrusive inspections. Rather, US willingness to compromise by accepting some level of enrichment in Iran was key to persuading Iran to accept limits. Without the compromise, there would have been no

deal[43]. Just weeks before President Biden was sworn into oce, Iran announced that it had increased its uranium enrichment levels to 20 percent, which broke the JCPOA's limit of 4 to 5 percent and brought it just one technical step away from weapons-grade levels.

The higher level of enrichment, authorized in the Iranian parliament, was the clearest sign that Iran is ready to disregard diplomacy and return to its dash for a bomb.

None of this was happening before President Trump reneged on the JCPOA without a viable path forward. Indeed, Trump's maximum pressure campaign of unilateral sanctions, travel restrictions on senior Iranian diplomats, and high-level Iranian assassinations have complicated governing and stressed Iran's economy. But, crucially, it has done nothing to stop Tehran from restarting its nuclear program, curtail its destabilizing behavior across the Middle East, and profoundly alienated our allies necessary for advancing our security objectives.

The Biden Administration has five scenarios for a future negotiation with Iran. The best outcome, reestablishing the JCPOA plus addressing regional activity and ballistic missile concerns, is also the most dicult to achieve. Iran has argued repeatedly that its ballistic missile program is non-negotiable. Nonetheless, it is the goal every US Administration should strive to reach.

The world is once again perilously close to staring down the possibility of a nuclear-armed Iran.

Securing a new deal to limit Iran's nuclear program plus follow-up negotiations for other issues is benecial for several reasons, including a true rebalance towards Asia and a stronger transatlantic alliance after years of neglect.

The politics of a new Iran deal are also good for Democrats. When President Obama signed the JCPOA in 2015, a majority of Americans supported the deal, and three years later, over 60 percent believed Trump should stay in the JCPOA.

More broadly, even after four years of Donald Trump's "America first" policies, almost 70 percent of Americans believe it is in the best interest of the United States to remain active in world affairs.

Still, Republican lawmakers are likely to reexively oppose any Biden deal with Iran even though halting Iran's nuclear program and striving toward more commitments would be a major accomplishment for American security[44]

Iran is reeling from the economic devastation of the COVID-19 pandemic. Iran has asked the International Monetary Fund for emergency funding, and arguments are now being made to suspend US sanctions.

In March 2020, the UK, France, and Germany conducted their first INSTEX transaction by exporting medical devices from Europe to Iran. In a press briefing, the French government reiterated the purpose of

[43] Fitzpatrick, M. (2017). Assessing the JCPOA. *Adelphi Series*, *57*(466-467), 19-60.

[44] Shilo, P., & Rosenblum, T. President Biden Has Five Options for Future Negotiations with Iran.

INSTEX: a solution to support legitimate trade between Europe and Iran in line with the JCPOA and UNSC Resolution 2231. The German government released similar statements and committed to work with STFI (Iran's SPV) on more transactions in the future.

The United States is the world leader in providing humanitarian aid. Iran's dire humanitarian needs make it difficult politically for the United States to maintain an anti-Iran stance (particularly vis-à-vis relations with European countries) but suspending its sanctions would be akin to opening Pandora's box. Relaxing trade sanctions and allowing Iran to trade in USD might allow the Iranian economy to recover as it fights a pandemic, but if Iran were allowed to freely trade in oil again, what would happen to the US's dream to be the largest oil exporter? Further, if the sanctions are relaxed beyond trade, would Iran also be able pursue its scientific (and perhaps nuclear) aspirations? Most importantly though, will lifting the sanctions be enough to stimulate the Irani economy and help them recover in a post COVID-19 world?

The confluence of growing resistance to US sanctions around the world, a global pandemic and humanitarian crisis, economic collapse, and an American election in November may throw the future of longtime US sanctions on Iran into doubt. Could this be the start of a new relationship between the United States and Iran[45]?

The Biden administration is still unclear on important new directions for its Middle East policy. In addition to a possible return to a nuclear deal with Iran, these include the withdrawal of American troops from Afghanistan and Iraq. Their long stay in the region has not provided the US with the desired results. But if Biden manages to complete his plans by the end of the year, a fundamentally different situation could arise in the Middle East. And such a situation is already forming when, through the mediation of Iraq, from where American troops are about to depart, a dialogue is established between America's main antagonist, Iran, and America's ally, Saudi Arabia. This raises questions, including those about the shale revolution. Does Biden's policy mean a US withdrawal from the Middle East? How much will this affect the strengthening of US adversaries' positions among those forces with which they have not been so successful in fighting? And finally, won't a new regional security system begin to form without the dominant American role[46]?

In conclusion, the landscape remains uncertain and unstable, even though there have already been indirect meetings in Vienna. The election of the ultra-conservative Ebrahim Raisi as President, who had strongly criticised the agreement concluded by Rouhani in 2015, does not appear to simplify a US re-entry into the JCPOA or an easing of Iran's position. What is certain is that after the US exit, the time it takes for Iran to

[45] Bootwala M. (2020), "The Iran Problem: An Evaluation of US Sanctions on Iran and Global Reaction", *Georgetown journal of international affairs,* Volume 21, pp. 136-141.

[46] Frolov, A. V. (2021). The Biden Administration and the Iran Nuclear Deal. *USA & Canada: ekonomika, politika, kultura*, (7), 48-62.

build a nuclear bomb has been drastically reduced, while the kilos of enriched uranium have increased considerably.

Chapter 3

Cryptocurrencies: understanding the phenomenon and its evolution

3.1 Origin of a digital currency and its working principles

Cryptocurrency is a digital or virtual currency that is still in its embryonic stage and has been gaining lots of attention worldwide. It has not replaced the government-issued money yet due to various factors inherent to it. However, the technological advances are filling the gaps and overcoming the current obstacles slowly and steadily. The reasons for the attention gained by cryptocurrencies during the past 10 years are multifold. First, it does not exist in a tangible or physical form. It is not a government-issued currency printable on paper. Cryptography is used to ensure its attributes to be used as a currency by which a cryptocurrency can be used as a medium of exchange and perform monetary transactions, in the same way as the printable bills can be used. Cryptography is the science by which intelligible data into or information can be scrambled or concealed by using encryption techniques. Encryption is done from the sender side to make the intelligible data into an unintelligible one. Whereas, on the receiver side, the decryption takes place to bring the encrypted data back into an intelligible form again. The processes of encryption and decryption take place via an algorithm. An algorithm stands for a set of instructions in the world of computing. These instructions in a computer programming language perform a specific task. Cryptocurrency derives its name from two words, namely, cryptography and currency; a digital currency controlled by cryptography. A cryptocurrency has no inherent value; however, its value comes from the people's belief in it. Considering cryptocurrency has no central or regulating authority; its value is defined by consensus from people believing in it. It is a borderless currency with which international payments can be made cheaper than conventional currencies. A conventional currency such as a U.S. dollar is governed by a central bank that defines its value represented by printable bills, coins, drafts, cheques, or other similar banking instruments[47].

The concept of digital money is around since the 1980s, but it took few decades to develop as a fully distributed solution.

One of the earliest attempts to create cryptocurrency started few decades back in the Netherlands. When a petrol station in the Netherlands suffered nighttime thefts, few developers tried to link money with newly designed smart cards. A user who needs to access the petrol station can use these smart cards instead of cash.

[47] Matharu, A. (2018), *Understanding cryptocurrencies: the money of the future*. New York: Business Expert Press.

This can be one of the earliest examples of electronic cash which might have led to the digital currency as we know them today[48].

On 31 October 2008, something happened that was noticed by probably no more than a few hundred people, but which was unique in its significance. An unknown person – or team of people – working under the pseudonym of Satoshi Nakamoto released a white paper with a technical proposal for a digital money system. It was of little interest to anyone outside a very small community of cryptography enthusiasts and computer scientists.

While many of these may have been excited by its potential, perhaps few would have predicted the headlines, wild rumours, hysteria, admiration and hatred that this idea has precipitated in the intervening years. Bitcoin is nothing more than software, publicly and freely available. When an individual downloads the software and begins running it, they are able to join a peer-to-peer network that allows payments to be sent around the world without the participants having to trust a bank or other financial service company[49].

The idea of transacting values without the need of a financial institution is a truly disruptive idea for the financial system. Note that in the absence of trust, the financial system faces systemic risk, that the whole system (not just one participant of the system) might collapse. Financial institutions also make sure that all transactions are recorded in a way that the double-spending problem is eliminated. So, anything that could emerge to challenge the way transactions services work should fulfill the main prerequisites of trust and double-spending avoidance. Satoshi Nakamoto's idea to create a cryptocurrency using the blockchain technology seemed to fulfill these two necessary requirements[50].

An early distinction was made between the protocol—using the capitalised term Bitcoin—and the tokens, which used the lower-case term bitcoin. New bitcoins are 'written into existence' by a network participant (a so-called miner) who has succeeded in transforming the format of a bundle of proposed transactions (of previously issued bitcoins, along with a single request to issue new ones as a reward) in such a way that the bundle can be hitched to a chain of previously hitched bundles. The word stem crypto within the term cryptocurrency might be seen as surrogate for cryptography, but could also have emerged from the cypherpunk movement, who identified "anonymous cash and other untraceable payment systems" as enabling feature within a crypto-anarchy. Bitcoin's mission of leveraging "cryptographic proof instead of trust" resonates with

[48] Panda, S. K., Elngar, A. A., Balas, V. E., & Kayed, M. (Eds.). (2020). *Bitcoin and Blockchain: History and Current Applications*. CRC Press.

[49] Lewis, R. (2020). *The cryptocurrency revolution: Finance in the age of bitcoin, blockchains and tokens*. Kogan Page, Limited.

[50] Daskalakis, N., & Georgitseas, P. (2020). *An introduction to cryptocurrencies: The crypto market ecosystem*. Routledge.

the above. Cryptography enters its architecture in various ways. A few examples are the integrity of, and consensus on a joint transaction history as well as the authorisation setup for sending tokens. However, the use of the surrogate crypto for Bitcoin is slightly arbitrary in the sense that earlier attempts at creating digital currencies relied heavily on cryptographic techniques as well. Nevertheless, it might seem justified by the fact that cryptography plays a far more central role for Bitcoin than it does for national currencies. Loosely speaking, the modern fiat monetary system consists of physical and digital credits—issued by state central banks, state treasuries, and private commercial banks—which circulate under a legal system that guarantees their redemption. The number of credits expands through issuance, after which they can be transferred in the course of exchange among those who use them, before being retired when they are returned to the issuers. This composite system of expandable-contractable credits is what we refer to as 'money' in everyday parlance. In this context, the term cryptocurrency is controversial, because—from its inception—the name has simply assumed that the tokens are money tokens. The controversy is amplified by the fact that enthusiasts sometimes use the term performatively to make the normative point that crypto tokens 'should be money', or—alternatively—to deny that what we currently call 'money' is in fact money. One strategy to negotiate these language politics is to initially strip the money assumption from the tokens by giving them the generic name crypto-tokens, and then listing their uncontroversial characteristics to compare them with fiat credits.

Tokens of early cryptocurrencies are data objects created through accounting, much like the act of typing out the number '1' creates the mental image of a 'thing'. This is what is referred to as a 'token', but they are 'blank tokens'. An example of a blank token in the physical world might be a clear plastic token with no inscription or rights attached to it. Bitcoin tokens, similarly, are empty signifiers, somewhat like the digital equivalent of blank physical tokens, but with strict supply limits. These blank digital tokens however, are promoted with a name and branded logo that serves as a mental image for them, without which they would be almost entirely featureless. The tokens can be said to be digital bearer instruments, in the sense that transfers can only be initiated by the possessor of a private key that can unlock an 'unspent transaction output'. The 'bearer-instrument-like' nature is one reason why cryptocurrency sometimes gets referred to as 'digital cash' (physical cash being the bearer-instrument form of fiat currency). The tokens move around—Bitcoin and some of its descendants are processing hundreds of thousands of transfers of tokens every day. Furthermore, they have a price measured in fiat currency and their tokens can be split into smaller pieces, or combined into larger ones. The fact that split-able and lump-able tokens with a fiat currency price can be moved gives the system a 'moneylike' feeling, and—under a shallow definition of money as something that is issued and moved around in association with commerce—the term cryptocurrency feels loosely plausible in everyday conversation. Most 'purchases' conducted with bitcoin tokens, however, take the form of countertrade. The token, priced in fiat currency, is compared to a good or service, priced in fiat currency, and from this comparison of two fiat currency prices emerges an exchange ratio between the token and the good or service. This is the conceptual

equivalent of superimposing a pair of two-way fiat currency transactions over each other and cancelling out the money flows, giving the residual appearance of the crypto-token being used as 'money' to 'pay' for a good or service. Nevertheless, Bitcoin is used primarily for speculation —buying the token with fiat currency with an intention to resell it for fiat currency—rather than using it to countertrade ('pay') for goods and services. This speculation drives volatility in the fiat currency price of tokens, which—when analysed through the lens of the conventional 'functions of money' paradigm favoured by economic textbooks (money as a medium-of-exchange, a store-of-value and a unit-of-account), poses problems for the 'moneyness' of the tokens. Not only are they not widely accepted in exchange for goods and services, but they are not widely used to price things, and attempts to provide prices are unintuitive. They also struggle to consistently 'store value' if we interpret that to mean 'maintain stable purchasing power' (which in the case of Bitcoin means 'maintain fiat price and countertrade ratios'). Put simply, while a person can generally predict how many bags of sugar US$ 100 will command in a month, they will be very uncertain as to how much sugar they can obtain through Bitcoin countertrade in a month[51].

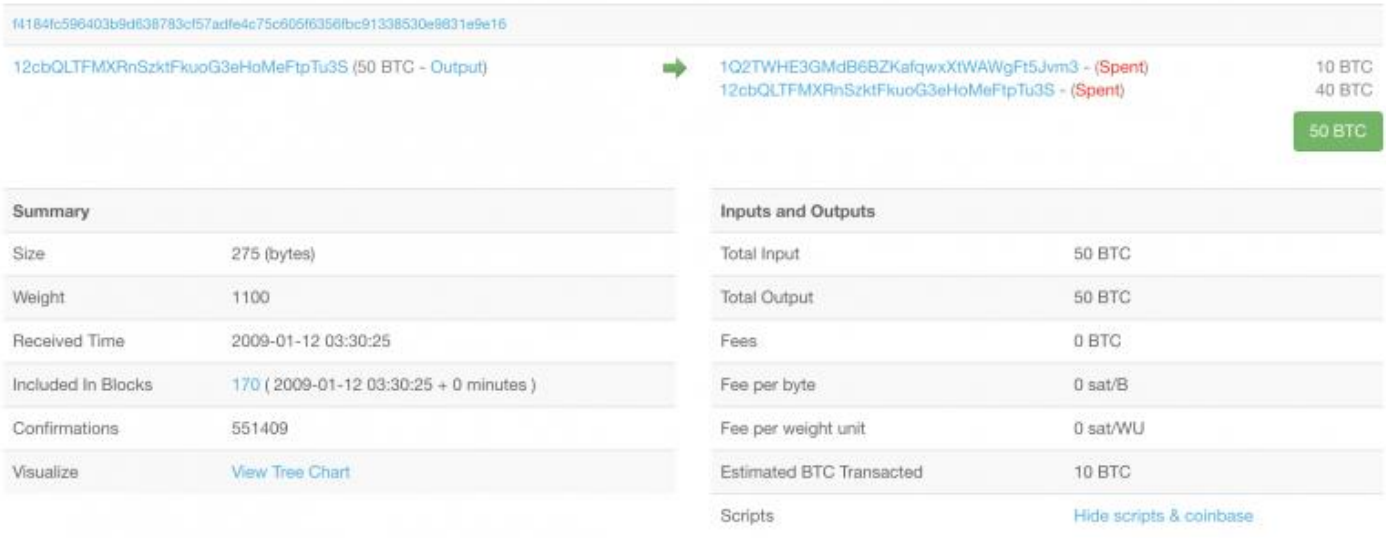


Figure 3.1 – First Bitcoin transaction

Source: Sedgwick K. (2018), "Eight historic Bitcoin transactions", Bitcoin.com, https://news.bitcoin.com/eight-historic-bitcoin-transactions/ , (viewed on 28/08/2021)

The question that most people ask is why Bitcoin has become so popular. It rose from the ashes of the financial crisis of 2008 to become a legitimate player in the global financial system. But what's all the excitement about, and why have people embraced digital currencies in general? The euphoria stems from the realization that Bitcoin could be the vehicle that transforms the financial system from centralized to decentralized. Our modern system of money transfer may be ostensibly based on bits and bytes, but at its core is an outdated centralized network of middlemen. Bitcoin is what is known as a decentralized distributed peer-to-peer network. This type

[51] Pernice, I. G. A., & Scott, B. (2021). Cryptocurrency. *Internet Policy Review, Glossary of decentralised technosocial systems, 10*(2).

of network allows people to transfer something of value without the expense of a middleman. Before the Western Union telegraph, the Pony Express was the only way to transfer information across the United States. Similarly, prior to e-mail and the Internet, the U.S. Postal Service had a virtual monopoly on information transfer. Bitcoin is about to do to the financial services industry what the telegraph did to the Pony Express and e-mail did to the U.S. Postal Service.

Three types of system are most common:

1. Centralized
2. Decentralized
3. Distributed

A centralized system can be thought of as a hub-and-spoke structure, where the key player sits in the middle and directs all the traffic. If the hub fails, the spokes fail as well. A decentralized system seeks to correct the flaw by creating multiple hubs and spokes. In a decentralized system, there are many nodes (or hubs), each charged with ensuring the smooth flow of traffic, whether the traffic is information, text messages, or financial transactions. A decentralized system is superior to the centralized system when preventing a failure at the hub is essential. There remains a risk that multiple hubs fail at the same time, but it is a step forward in the evolution of systems. It is also particularly useful when each hub can act autonomously. The next evolution is a distributed system, where every player acts as a hub. Each individual, business, computer, or government all have the same responsibility – ensure the smooth functioning of the system. In a distributed system, if one nod (or hub) fails, the other nodes simply pick up the slack and make sure traffic flows smoothly. A distributed system works best when the decision-making process can be automated or coded into a series of yes/no questions. If each node is responsible for the same output then the decision-making process must be identical. The revolutionary accomplishment of Satoshi Nakamoto was to reduce the complicated tangle of global finance middlemen into an elegant software package that can be downloaded onto a smartphone. This feat is not just astounding – it is unprecedented[52].

[52] Kelly, B. (2014). *The bitcoin big bang: How alternative currencies are about to change the world* (1st ed.). Wiley.

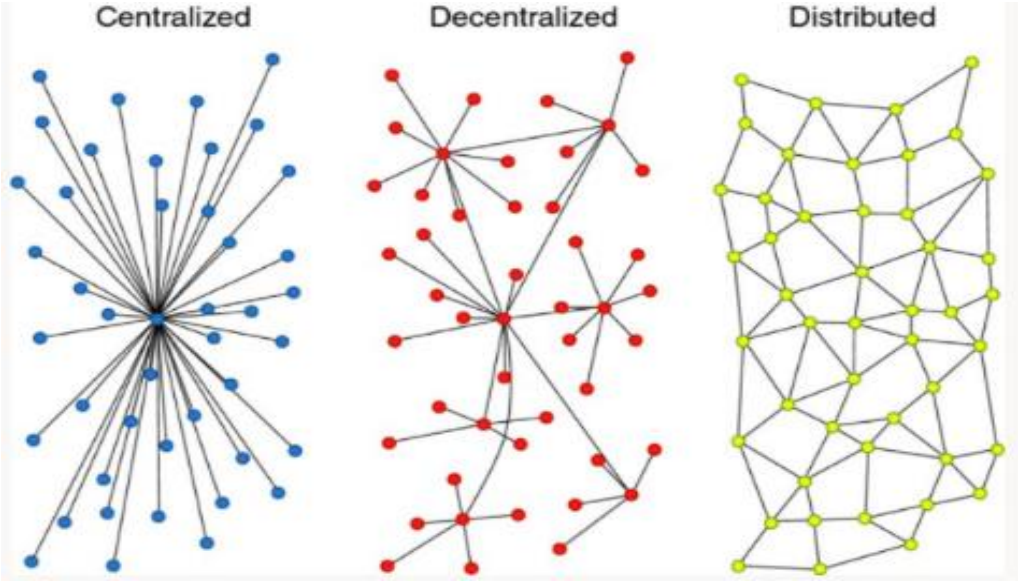


Figure 3.2 – Types of system

Source: Kelly, B. (2014). *The bitcoin big bang: How alternative currencies are about to change the world* (1st ed.). Wiley.

3.1.1 Blockchain

A blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. Bitcoin is the most popular example that is intrinsically tied to blockchain technology. It is also the most controversial one since it helps to enable a multibillion-dollar global market of anonymous transactions without any governmental control. Hence it has to deal with a number of regulatory issues involving national governments and financial institutions. However, Blockchain technology itself is non-controversial and has worked flawlessly over the years and is being successfully applied to both financial and non-financial world applications.

Current digital economy is based on the reliance on a certain trusted authority. All online transactions rely on trusting someone to tell us the truth— it can be an email service provider telling us that our email has been delivered; it can be a certification authority telling us that a certain digital certificate is trustworthy; or it can be a social network such as Facebook telling us that our posts regarding our life events have been shared only with our friends or it can be a bank telling us that our money has been delivered reliably to our dear ones in a remote country. The fact is that we live our life precariously in the digital world by relying on a third entity for the security and privacy of our digital assets. The fact remains that these third-party sources can be hacked, manipulated or compromised. This is where the blockchain technology comes handy. It has the potential to revolutionize the digital world by enabling a distributed consensus where each and every online transaction

involving digital assets, past and present, can be verified at any time in the future. It does this without compromising the privacy of the digital assets and parties involved. The distributed consensus and anonymity are two important characteristics of blockchain technology. Blockchain technology is finding applications in wide range of areas; both financial and non-financial. Financial institutions and banks no longer see blockchain technology as a threat to traditional business models. The world's biggest banks are in fact looking for opportunities in this area by doing research on innovative blockchain applications. Non-Financial applications opportunities are also endless. We can envision putting proof of existence of all legal documents, health records, and loyalty payments in the music industry, notary, private securities and marriage licenses in the blockchain. By storing the fingerprint of the digital asset instead of storing the digital asset itself, the anonymity or privacy objective can be achieved. We explain the concept of the blockchain by explaining how Bitcoin works since it is intrinsically linked to the Bitcoin. However, the blockchain technology is applicable to any digital asset transaction exchanged online. Bitcoin uses cryptographic proof instead of the trust-in-the-third-party mechanism for two willing parties to execute an online transaction over the Internet. Each transaction is protected through a digital signature, is sent to the "public key" of the receiver, and is digitally signed using the "private key" of the sender. In order to spend money, the owner of the cryptocurrency needs to prove his ownership of the "private key". The entity receiving the digital currency then verifies the digital signature, which implies ownership of the corresponding "private key", by using the "public key" of the sender on the respective transaction. Each transaction is broadcasted to every node in the Bitcoin network and is then recorded in a public ledger after verification. Every single transaction needs to be verified for validity before it is recorded in the public ledger. The verifying node needs to ensure two things before recording any transaction:

1. Spender owns the cryptocurrency, through the digital signature verification on the transaction.

2. Spender has sufficient cryptocurrency in his account, through checking every transaction against the spender's account, through checking every transaction against the spender's account, or "public key", that is registered in the ledger. This ensures that there is sufficient balance in his account before finalizing the transaction.

However, there is question of maintaining the order of these transactions that are broadcasted to every other node in the Bitcoin peer-to-peer network. The transactions do not come in order in which they are generated, and hence there is a need for a system to make sure that double-spending of the cryptocurrency does not occur. Considering that the transactions are passed node by node through the Bitcoin network, there is no guarantee that orders in which they are received at a node are the same order in which these transactions were generated. The above means that there is a need to develop a mechanism so that the entire Bitcoin network can agree regarding the order of transactions, which is a daunting task in a distributed system. The Bitcoin solved this problem by a mechanism that is now popularly known as Blockchain technology. The Bitcoin system orders

transactions by placing them in groups called blocks and then linking these blocks through what is called Blockchain. The transactions in one block are considered to have happened at the same time. These blocks are linked to each-other (like a chain) in a proper linear, chronological order with every block containing the hash of the previous block. There still remains one more problem: Any node in the network can collect unconfirmed transactions and create a block and then broad cast it to the rest of the network as a suggestion as to which block should be the next one in the blockchain. How does the network decide which block should be next in the blockchain? There can be multiple blocks created by different nodes at the same time. One can't rely on the order since blocks can arrive at different orders at different points in the network. Bitcoin solves this problem by introducing a mathematical puzzle: each block will be accepted in the block chain provided it contains an answer to a very special mathematical problem. This is also known as "proof of work": a node generating a block needs to prove that it has put enough computing resources to solve a mathematical puzzle. For instance, a node can be required to find a "nonce" which when hashed with both transactions and hashes of previous blocks produces a hash with certain number of leading zeros. The average effort required is exponential in the number of zero bits required but verification process is very simple and can be done by executing a single hash.[53].

The core ideas behind blockchain technology emerged in the late 1980s and early 1990s. In 1989, Leslie Lamport developed the Paxos protocol, and in 1990 submitted the paper The PartTime Parliament to ACM Transactions on Computer Systems; the paper was finally published in a 1998 issue. The paper describes a consensus model for reaching agreement on a result in a network of computers where the computers or network itself may be unreliable. In 1991, a signed chain of information was used as an electronic ledger for digitally signing documents in a way that could easily show none of the signed documents in the collection had been changed. These concepts were combined and applied to electronic cash in 2008 and described in the paper, Bitcoin: A Peer-to-Peer Electronic Cash System, which was published pseudonymously by Satoshi Nakamoto, and then later in 2009 with the establishment of the Bitcoin cryptocurrency blockchain network[54].

The initial excitement about blockchain technology was about enabling peer-to-peer transfers of digital currency to anybody in the world, crossing human-created boundaries without any intermediaries such as bank. This excitement was further heightened by the realization that this peer-to-peer capability could be applied to other, non-cryptocurrency types of transactions. These transactions involve assets such as titles, deeds, music and art, secret codes, contracts between businesses, autonomous driver decisions, and artifacts resulting from

[53] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.

[54] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

many contain other details based on the blockchain protocol and the application. Following its initial success, people began to ask, "If you can transact digital currency, why not any other digital assets?" This question was answered around 2013 with the addition of an environment for code execution on another popular blockchain, Ethereum. The innovation was that the verification, validation, and recording could be extended to other digital assets and to related transactions and systems. Therefore, blockchain can play a crucial role in implementing decentralized systems by providing software-based intermediation to other (non-currency) peer-to-peer transactions[55].

Another relevant element, which allows us to better understand the blockchain mechanism, is the hash.

A hash is a short code of defined length which serves as a fingerprint for a digital document. A program called a hash-generator allows a user to upload any string of text 38 and create a unique ID. Every time the same string of text is run through the hash generator, it will give the same document-ID. The contribution of hashing as an antitampering device is significant: if a single letter in a document is changed, it will automatically generate a completely different ID. Hashes are one-way. This means that the hash-generator can be used to generate a hash from the document, but it is mathematically impossible to generate a document from a hash. In a blockchain, each block of transactions is secured by including a hash of the information block, as well as of the previous block, thus allowing all parties to guarantee that none of the transactions has been modified or tampered with[56].

[55] Ramamurthy, B. (2020). *Blockchain in action.* Manning Publications.

[56] Grech, A., & Camilleri, A. F. (2017). *Blockchain in education*. Luxembourg: Publications Office of the European Union.

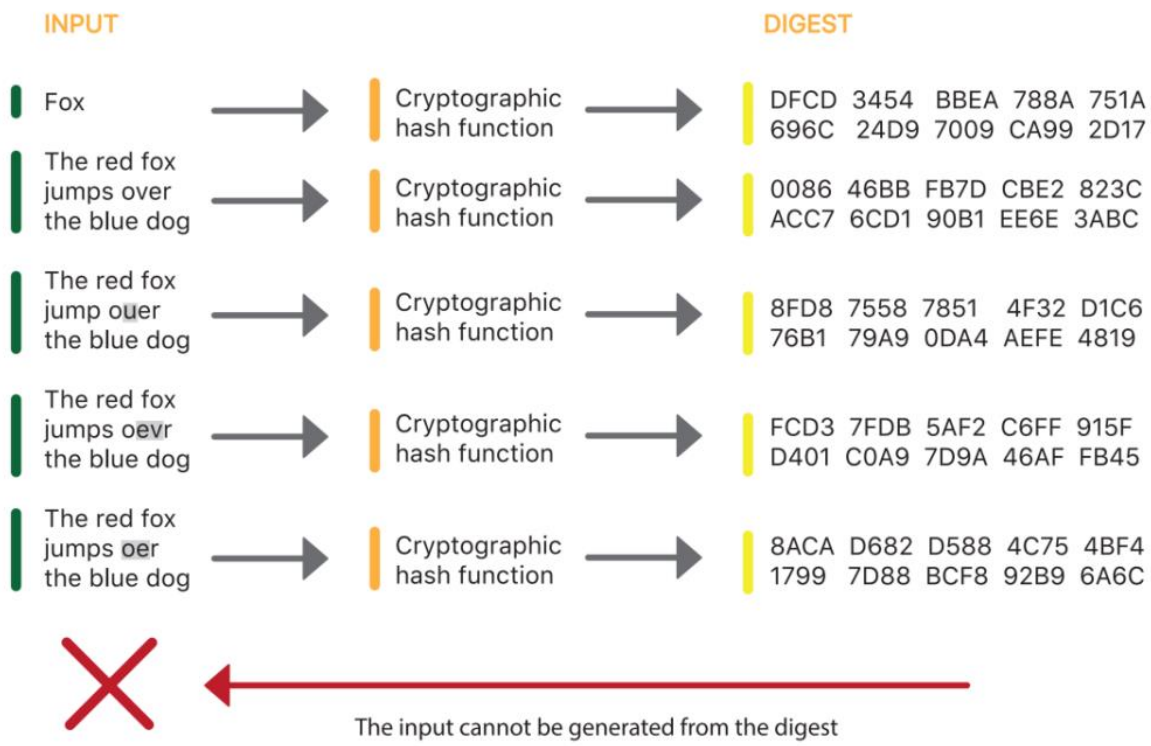


Figure 3.3 – Cryptographic hash function

Source: Adapted from: https://commons.wikimedia.org/wiki/File:Hash_function.svg

In addition, immutability is also important. Immutability refers to anything and everything that cannot be changed once recorded. For example, a mail sent to a bunch of people cannot be reversed. An additional field called timestamp is stored inside the block when a transaction is approved and appended onto the blockchain. If anyone tries to alter the data in a block the cryptographic link is broken. This helps us to recognize the precise section of the chain where the data is manipulated. Thus, one has to compute the previous hash value of the entire chain again to restore the link. It requires a lot of computational power in order to do so. Therefore, making sure that the data stored is resistant to any kind of alterations. This feature is not available in the earlier databases which only provide an option to delete or modify records. Moreover, blockchains sustain the entire history and data path of any application. This acts as a backbone for any auditing process. Preserving a full historical record is not only a blessing for auditing, but also provides new chances in the query, analytics, and overall business processes. The backbone of blockchain methodology is formed by P2P network architecture. This policy authorizes us to remove the dependency on a central decision-making source called a server. The user has to completely trust networks and hope they don't have a backdoor to quietly read or manipulate the reports. Also, one should hope that they don't go out of business and shut down their servers. The nodes comprising tablets, routers, etc., interact and share data directly with one another; thus, distributing all the data across all nodes in the grid rather than using a server. All the nodes in the network will have a copy of the blockchain, thereby making it completely impossible for anyone to modify any value in the chain. Hypothetically, all these nodes are joined via a path. None of the nodes have precise knowledge about the

network topology and merely reroute messages to the designated node. Members of the P2P network share the resources between other members, including bandwidth, disk storage, etc. This is accomplished with the help of minimum resource contribution threshold defined for all peers in the network. The peer-to-peer network enables us to solve all the obstacles faced in client-server architecture, i.e., single source of failure and scalability, efficiently[57].

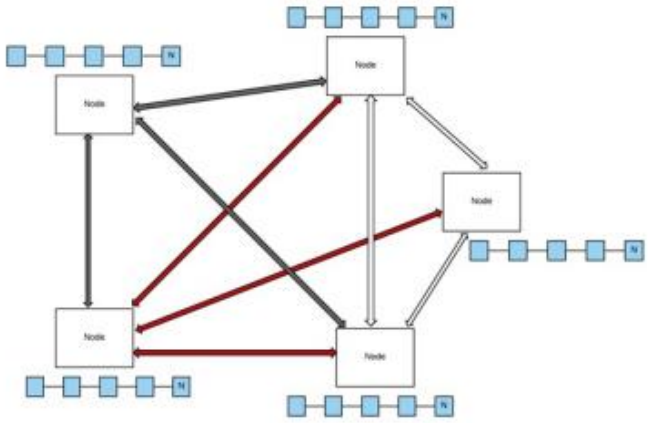


Figure 3.4 – P2P network of blockchain

Source: Gururaj, H. L., Manoj Athreya, A., Kumar, A. A., Holla, A. M., Nagarajath, S. M., & Ravi Kumar, V. (2020). Blockchain: A new era of technology. *Cryptocurrencies and Blockchain Technology Applications*, 1-24.

3.1.2 Smart contracts

The term "smart contract" was first coined in mid1990s by computer scientist and cryptographer Szabo, who defined a smart contract as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises. Generally speaking, smart contracts can be defined as the computer protocols that digitally facilitate, verify, and enforce the contracts made between two or more parties on blockchain. As smart contracts are typically deployed on and secured by blockchain, they have some unique characteristics. First, the program code of a smart contract will be recorded and verified on blockchain, thus making the contract tamper-resistant. Second, the execution of a smart contract is enforced among anonymous, trustless individual nodes without centralized control, and coordination of third-party authorities. Third, a smart contract, like an intelligent agent, might have its own cryptocurrencies or other digital assets, and transfer them when predefined conditions are triggered. It is worth noting that Bitcoin is widely recognized as the first cryptocurrency that support basic smart contracts, in the sense that its transactions will be validated only if

[57] Gururaj, H. L., Manoj Athreya, A., Kumar, A. A., Holla, A. M., Nagarajath, S. M., & Ravi Kumar, V. (2020). Blockchain: A new era of technology. *Cryptocurrencies and Blockchain Technology Applications*, 1-24.

certain conditions are satisfied. However, designing smart contract with complex logic is not possible due to the limitations of Bitcoin scripting language that only features some basic arithmetic, logical, and crypto operations.

Ethereum is the first public blockchain platform that supports advanced and customized smart contracts with the help of Turing-complete virtual machine called Ethereum virtual machine (EVM). Smart contracts are introduced as computer programs running across the blockchain network and can express triggers, conditions, and business logic to enable complicatedly programmable transactions[58].

There are two types of smart contracts, namely, deterministic and non-deterministic smart contracts. A deterministic smart contract is a smart contract that when it is run, it does not require any information from an external party (from outside the blockchain). A non-deterministic smart contract is a contract that depends on information (called oracles or data feeds) from an external party. For example, a contract that requires the current weather information to be run, which is not available on the blockchain. There are various possible applications where smart contracts can be applied to. Some of these applications are as follows:

- Internet of Thing and smart property: there are billions of nodes that are sharing data between each other through the Internet. A potential use case of blockchain-based smart contracts is to allow those nodes to share or access different digital properties without a trusted third party. There are various companies that investigate this use case. For example, Slock.it is a German company that utilises Ethereum-based smart contracts for renting, selling or sharing anything (e.g, selling a car) without the involvement of a trusted third party.

- Music rights management: a potential use case is to record the ownership rights of a music in the blockchain. A smart contract can enforce the payment for music owners once a music is used for commercial purposes. It also ensures the payment is being distributed between the music's owners. Ujo is a company that investigates the use of blockchain-based smart contracts in the music industry.

- E-commerce: a potential use case is to facilitate the trade between untrusted parties (e.g., seller and buyer) without a trusted third party. This would result in reduction of trading costs. Smart contracts can only release the payment to the seller once the buyer is satisfied with the product or service they received. There are other

[58] Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(11), 2266-2277.

possible applications such as e-voting, mortgage payment, digital right management, motor insurance, distributed file storage, identity management and supply chain[59].

The smart contracts facilitate the enforcement of contractual agreements with in-built transparency and forge resistance. The distinguishing features of smart contracts make it pertinent into many applications. A lot of research conducted in the industry as well as academia in order to investigate the strengths and applicability of smart contracts in different application domains. Furthermore, the improvements of technical aspects highly focused to fine tune the smart contracts for the enhancement of compatibility of the smart contracts. There are many smart contract platforms emerging in the market with associated distinguishing features which suits for specific applications. Smart contracts can transform the business rules into the computer programs. Different smart contract platforms have developed to address specific requirements in each industry. Each smart contract platform includes a set of specific features targeted to the particular application[60].

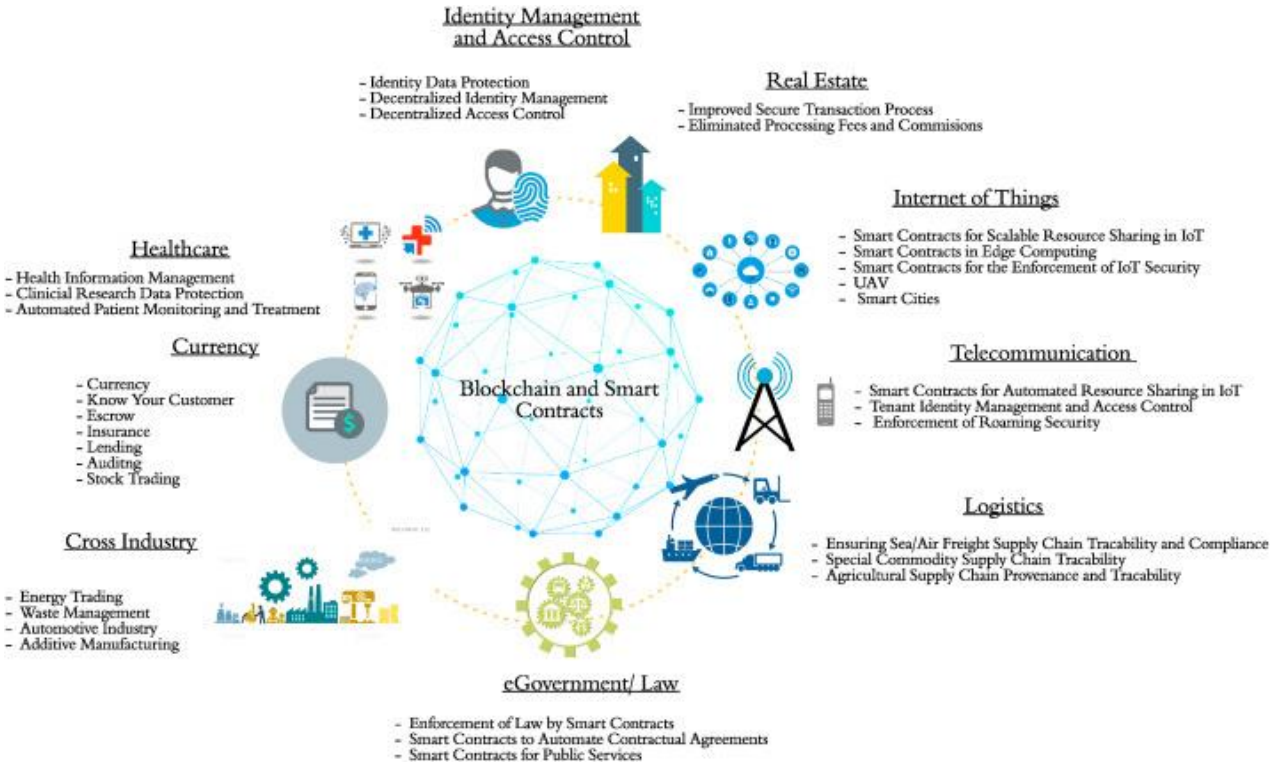


Figure 3.5 – Different smart contract applications

Source: Hewa, T., Ylianttila, M., & Liyanage, M. (2020). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, 102857.

[59] Alharby, M., & Van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. *arXiv preprint arXiv:1710.06372*.

[60] Hewa, T., Ylianttila, M., & Liyanage, M. (2020). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, 102857.

3.1.3 The impact of cryptocurrency mining

This section aims to analyse the health and environmental impact of the mining process of four cryptocurrencies using proof-of-work. The cryptocurrencies examined are the following: Bitcoin, Ethereum, Litecoin and Monero. Miners provide their own computers and electricity in order to mine cryptocurrencies and be rewarded for doing so. Mining is done by solving complex algorithms to provide the hash identifier for a block. If successful, miners are rewarded with one or more cryptocurrency units and the data of new transactions are verified by network users and then added to the blockchain.

To add a block (i.e., a collection of transaction data) to the blockchain, a miner has to solve a cryptographic puzzle based on the block. This mechanism prevents malicious nodes from trying to add bogus blocks to the blockchain and earn the reward illegitimately. A valid block in the blockchain contains a solution to a cryptographic puzzle that involves the hash of the previous block, the hash of the transactions in the current block, and a wallet address to credit with the reward. The cryptographic puzzle is designed such that the probability of finding a solution for a miner is proportional to the miner's computational power. Due to the nature of the mining process, the interval between mining events exhibits high variance from the point of view of a single miner. Consequently, miners typically organize themselves into mining pools. All members of a pool work together to mine each block, and share the reward when one of them successfully mines a block[61].

While alternatives exist, cryptocurrency applications using blockchain remain dominated by the proof-of-work (POW) process used in the original Bitcoin, where the probability of successful mining is increased by the amount of computing work expended. Thus, mining generates financial value, but consumes electricity in doing so. The complication is that the supply of any cryptocurrency coin is typically finite and made available according to prescribed rules that asymptotically approach some fixed amount at a specified point in time. Specifically, as the supply of new coins slows, the implication of a POW process is that the competing computing effort to mine coins must necessarily increase, thus requiring ever increasing amounts of electricity. Thus, the "strange math" of cryptocurrency provision based on a POW process generates intense electricity resource use, potentially creating negative—and growing—environmental and health costs that may be high and are not borne by the miners. As with any emergent technology, there needs to be careful consideration of its environmental and health impacts on society. In the emerging literature considering these impacts, Krause and Tolaymat push such assessments significantly forward by quantifying the energy and carbon emissions for mining four prominent cryptocurrencies (Bitcoin (BTC), Ethereum (ETH), Litecoin (LTE), and Monero

[61] Konoth, R. K., Vineti, E., Moonsamy, V., Lindorfer, M., Kruegel, C., Bos, H., & Vigna, G. (2018, October). Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1714-1730).

(XMR), all identified as using a POW process). They pursue the following questions: (i) do these cryptocurrencies require a similar energy supply to function?; (ii) what conventional processes or services would "cryptomining" compared to (e.g., gold mining), in terms of energy invested and value extracted?; and (iii) what carbon impacts might this energy consumption generate? They find that cryptomining of BTC, ETH, LTC, and XMR tends to consume more energy than traditional mineral mining such as copper, gold, platinum metals, and rare earth metals (with the exception of aluminum, which has high electricity consumption) in producing an equivalent market value. Their results additionally indicate that energy consumption requirements are generally expected to increase, for reasons previously discussed, and that BTC consumed more electricity than Ireland (26 TWh yr^{-1}) or Hong Kong (44 TWh yr^{-1}) in 2017. Finally, for the 2.5-year period (January 1, 2016 to June 30, 2018), they estimate that the four prominent cryptocurrencies were responsible for 3 – 15 million tonnes (t) of CO_2 emissions. The electricity consumption of mining cryptocurrencies is large and growing rapidly. For example, in January of 2016, each BTC mined required 1005 kWh of electricity; but by June 2018, each coin mined required 60,461 kWh. In 2016 there were ~1 million BTC mined, which consumed 2.5 billion kWh of electricity; in 2018 the total number of coins mined dropped to 700,000, but electricity consumption increased to 47.9 billion kWh. This usage creates negative social externalities, most significantly by contributing to climate change and impacting human health from the burning of fossil fuels. It was recently argued that CO_2 emissions from Bitcoin mining alone could push global warming above the 2 °C threshold of concern. Economists use a battery of techniques to estimate the monetary damages connected to these non-market negative externalities, which by definition are not accounted for in the market production or consumption of a good or service. For the US and China, our main finding is that in 2018, each $1 of Bitcoin value created was responsible for $0.49 in health and climate damages in the US and $0.37 in China. Put differently, the human health and climate damages caused by Bitcoin represented *almost half* of the financial value of each US dollar of Bitcoin created (as represented by market prices). Further, the slightly smaller value in China relative to the US (for each $1 of Bitcoin created) occurs primarily due to the extremely large disparity between the VSL estimate for the US ($11.53 million) relative to that of China ($1.12 million), a more than 10-to-1 ratio. If the energy demand timelines for producing Ethereum, Litecoin, and Monero follow Bitcoin, then we might anticipate similar per dollar health and climate damages in the near future. It is also clearly possible in the prescribed supply rules for a cryptocurrency that the *crypto damages*—the human health and climate impacts—will eventually exceed each $1 value created. The above estimates ($0.49 in the US and $0.37 in China) are averaged over the year (2018); but, notably averaged across December 2018 we observed each $1 of BTC value created, generated $0.95 of crypto damages in the US. For any cryptocurrency tied to the POW process (or something similar), the rising electricity requirements to produce a single coin leads to a situation where the price must continue rising, faster than the social costs, to maintain positive net benefits for society. Without perpetual price increases, coin mining may follow an almost

inevitable cliff of negative net social benefits as the energy use required for mining increases by greater and greater amounts due to the POW process[62].

Table 3.1 – Mortality impacts, climate damages, and health damages of coin mining created by country, year, and cryptocurrency.

		Mortality per million coins		Climate damages ($ per coin)		Health damages ($ per coin)		Damages (% of coin value)		Global coins mined (millions)
		USA	China	USA	China	USA[a]	China[b]	USA	China	
BTC	2016	4.6	9.6	74	86	53	11	21%	16%	1.0
	2017	19	40	311	359	222	45	19%	14%	0.70
	2018	115	239	1849	2135	1321	268	49%	37%	0.68
ETH	2016	0.03	0.06	0.49	0.57	0.35	0.07	9%	7%	10.8
	2017	0.59	1.2	9.5	11	6.8	1.4	8%	6%	8.7
	2018	2.5	5.2	40	46	29	5.8	21%	16%	6.6
LTC	2016	0.01	0.02	0.15	0.17	0.10	0.02	7%	5%	5.3
	2017	0.08	0.16	1.22	1.4	0.87	0.18	5%	4%	5.4
	2018	0.94	2.0	15.2	18	11	2.2	37%	28%	5.3
XMR	2016	0.02	0.05	0.35	0.41	0.25	0.05	27%	21%	3.1
	2017	0.19	0.39	3.0	3.5	2.2	0.44	8%	6%	1.9
	2018	1.0	2.1	17	19	12	2.4	22%	17%	1.1

Notes: BTC = Bitcoin, ETH = Ethereum, LTC = Litecoin, XMR = Monero. Mortality impacts associated with power plant emissions of $PM_{2.5}$, SO_2, and NO_x due to country and year-specific cryptocurrency mining activity. All damages are in 2018 US Dollars.

a: Health damages in US calculated with $11.53 million VSL.

b: Health damages in China calculated with $1.12 million VSL.

Source: Goodkind, A. L., Jones, B. A., & Berrens, R. P. (2020). Cryptodamages: Monetary value estimates of the air pollution and human health impacts of cryptocurrency mining. *Energy Research & Social Science*, *59*, 101281.

[62] Goodkind, A. L., Jones, B. A., & Berrens, R. P. (2020). Cryptodamages: Monetary value estimates of the air pollution and human health impacts of cryptocurrency mining. *Energy Research & Social Science*, *59*, 101281.

In the past few years, cryptocurrencies have increasingly attracted the attention of users and investors. As things currently stand, Bitcoin and other altcoins are used as a speculative investment tool and the major change that is being brought about by cryptocurrencies is being ignored. This study examined the environmental dimensions of Bitcoin mining as the first cryptocurrency in terms of both its market value and volume. It is understood that nearly 80% of global energy consumption is through fossil fuels, that this view is not likely to change in the short term, and that fossil fuels will continue to be important in the future. Despite the important developments in alternative energy sources, it is obvious that the energy needs of the global economy is dependent in large part on the hydrocarbon sector. It is with this perspective in mind that the energy used up by miners during the processes of confirming Bitcoin transactions, recording them, and producing Bitcoin has been examined here. It has been emphasized that as a result of the extreme need for computer power in order to mine Bitcoin, the astronomical amount of energy used is not sustainable. The day-by-day increase in the use of energy for Bitcoin has meant that it uses up more energy than many countries and that it harbors many dangers for Bitcoin's future. It is known that in order to avoid the high energy costs of Bitcoin mining, individuals and firms have been carrying out these operations in countries where energy is low-cost. The energy required by Bitcoin transactions and mining, which are obtained from coal and thermal plants – hydrocarbons – result in increased CO2 emissions and cause a rise in global warming, air pollution, and even death rates. The sustainability of the environment is important for the world's development and growth, and as depicted in the Paris Climate Agreement, precautions must be taken against global warming and climate change. During such a time, the magnitude of Bitcoin's energy consumption causes serious damage to the environment and faces us as one of the most significant obstacles in the development of Bitcoin[63].

3.2 Evolution and growth of the cryptomarket

The financial market universe comprises a wide set of assets that offer potential investors almost countless investment opportunities. New financial assets and instruments are formulated or developed periodically, which ultimately attracts capital and attention. The latest example is the cryptocurrency market, which started in 2009 with the then exotic, relative, and mysterious—but now well-known—Bitcoin. However, nonprofessionals are most likely not aware of the exponential expansion of the number of traded cryptocurrencies. To gauge this expansion, the following can be considered. At the birth of the cryptocurrency market, the number of cryptocurrencies was equal to one and remained at that level until April 17, 2011.

[63] Dilek, Ş., & Furuncu, Y. (2019). Bitcoin mining and its environmental effects. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi*, *33*(1), 91-106.

Subsequently, the number of traded cryptocurrencies started to soar, reaching the value of 50 on August 4, 2013, while it increased to 500 by October 26, 2014, and further increased to 1500 by February 25, 2018; it currently (as of June 14, 2020) stands at 2,670 traded cryptocurrencies (source: CoinMarketCap). In other words, since its birth, the cryptocurrency market has exhibited a 266,900% increase in terms of the number of traded currencies. It is difficult to think of another economic and/or financial phenomenon with an equivalent increase rate over a decade, possibly with the exceptions of the Tulip Mania (1619–1622) and the Mississippi Bubble (1716–1719)[64].

In recent years, cryptocurrencies have been in the spotlight of attention in financial markets all over the world. Bitcoin, which was the first currency of this technology to be invented, still remains the most popular digital currency; however, other alternatives such as Ethereum and Ripple are gaining pace, while in fact, during 2017, the market capitalization of all other digital currencies put together had equated the capitalization of Bitcoin. Unequivocally, increased interest in cryptocurrencies rests largely upon the fact that their applications have the potential to determine future developments in many important aspects of real economic activity. For instance, Yermack (2018) puts forward the argument that the Bitcoin, although vulnerable to speculation, is widely being used as an alternative to fiat money, while blockchain technology in general, might very well affect both central banking and corporate governance[65].

After Bitcoin appeared in 2009, approximately 1500 other cryptocurrencies have been introduced, about 600 of which are actively traded today. All cryptocurrencies share the underlying blockchain technology and reward mechanism, but they typically live on isolated transaction networks. Many of them are basically clones of Bitcoin, although with different parameters such as different supplies, transaction validation times, etc. Others have emerged from more significant innovations of the underlying blockchain technology. Between 2.9 and 5.8 million of private as well as institutional users actively exchange tokens and run the various transaction networks. In May 2017, the market capitalization of active cryptocurrencies surpassed $91 billion. Bitcoin currently dominates the market, but its leading position is challenged both by technical concerns and by the technological improvements of other cryptocurrencies. Bitcoin was introduced in 2009 and followed by a second cryptocurrency (Namecoin) only in 18 April 2011. This first-mover advantage makes Bitcoin the most famous and dominant cryptocurrency to date. However, recent studies analysing the market shares of Bitcoin and other cryptocurrencies reached contrasting conclusions on its current state. While Gandal and Halaburda in their 2016 study concluded that ‘Bitcoin seems to have emerged, at least in this stage, as the

[64] Ballis, A., & Drakos, K. (2021). The explosion in cryptocurrencies: a black hole analogy. *Financial Innovation*, *7*(1), 1-8.

[65] Antonakakis, N., Chatziantoniou, I., & Gabauer, D. (2019). Cryptocurrency market contagion: Market uncertainty, market complexity, and dynamic portfolios. *Journal of International Financial Markets, Institutions and Money*, *61*, 37-51.

clear winner', the 2017 report by Hileman and Rauchs noted that 'Bitcoin has ceded significant market cap share to other cryptocurrencies'[66].

3.3 The governance of cryptocurrencies

While the technological structure of distributed ledger-based cryptocurrencies makes them resistant to fraud or theft, the direct democratic approach to cryptocurrency governance is a considerable challenge to cryptocurrency's transparency, sustainability, and decision making in the near future. The lack of a central administrator makes it difficult to overcome technological challenges of increasing demand and currency growth (i.e., scalability challenges) by developing and adopting changes to a cryptocurrency's platform technology. Currently, many cryptocurrencies like Bitcoin possess a decentralized style of governance whereby updates to the currency's software protocol are determined by a consensus of the network's participants. Although this process normally operates with minimal disruption, entrenched disagreements between differing factions within Bitcoin's governance process can generate a rift in the cryptocurrency's user base. Among the more famous examples of this includes the Summer 2017 rift that split the Bitcoin community into two rival blockchains—Bitcoin and Bitcoin Cash. The demonstrated potential for such rifts is a clear challenge to effective cryptocurrency governance that, if not properly predicted and ameliorated, can reduce trust, and use by the public—something critical to cryptocurrency success in the marketplace. Such concerns are particularly salient for the scaling challenge facing many cryptocurrencies like Bitcoin, where software improvements are needed to increase the number of transactions that the cryptocurrency's network can process per block. As usership for Bitcoin and other cryptocurrency's has grown significantly in 2017–2018, increasing demand for limited space in each block has increased transaction fees and transaction time in a manner that threatens the feasibility of such cryptocurrencies altogether[67].

The technical infrastructure Nakamoto outlined for Bitcoin implies a non-technical governance structure with different actors. The nature of the system itself distributes technical power, forming the basis for decentralized governance. The cryptocurrency system is defined by several key stakeholders that each carry a crucial function: users, who choose to send and receive payments on the blockchain network; miners, who both verify transactions and mine new coins at a preordained rate set by the system to keep the money supply consistent; developers, who create and update the system; and finally, external stakeholders, such as non-profit

[66] ElBahrawy, A., Alessandretti, L., Kandler, A., Pastor-Satorras, R., & Baronchelli, A. (2017). Evolutionary dynamics of the cryptocurrency market. *Royal Society open science*, *4*(11), 170623.

[67] Trump, B. D., Wells, E., Trump, J., & Linkov, I. (2018). Cryptocurrency: governance for what was meant to be ungovernable. *Environment Systems and Decisions*, *38*(3), 426-430.

foundations, wallets, and currency exchanges, that affect the funding and development of cryptocurrency. The promise of cryptocurrency thus fundamentally does not entirely eliminate governance, but redefines it from traditional employer/employee or contractual relationships toward trust less, virtual interactions that attempt to reduce the existence of formal governance structures. Furthermore, despite the novelty of cryptocurrency's technical infrastructure, recent developments indicate that governance may play a larger role than anticipated by cryptocurrency creators. Analysis of both Bitcoin and Ethereum reveals that both cryptocurrencies have rich and developed non-technical governance structures that are crucial to their success. A descriptive overview of each cryptocurrency reveals that while each proposes a unique technical system to eliminate the need for TTPs (trusted third parties), neither truly succeeds in eliminating the potential powers of stakeholders. In Bitcoin, the rise of mining pools and the ability of users to use external financial instruments to manipulate the price and profit gains create strong motivation to take over the system. In Ethereum, the precedent set by developers in rejecting the DAO (Decentralized Autonomous Organization) and forcing a hard fork has created both the perception and potential for core developers to dictate the direction and composition of the system. In both cryptocurrencies, a lack of formalized structure in adapting to changes and accepting input from multiple stakeholders internal and external to the system has resulted in periods of instability. Despite the potential for manipulations, both Bitcoin and Ethereum remain relatively popular. Their systems are utilized at a high rate across all stakeholder groups, and there remains to be a tremendous amount of excitement around the long term and lasting consequences on the ways that transactions can be processed on each system. Among cryptocurrencies, both Bitcoin and Ethereum have generated strong followings that indicate they have community support and potential to succeed. Furthermore, despite forking events and security concerns, the majority of potential power usurpations have not been undertaken on the network. For example, mining pools have existed and continued to grow without system-wide repercussions for Bitcoin, and DAOs continue to proliferate and seek funding in Ethereum. The relative success of these cryptocurrencies despite the demonstrated weaknesses in their technical interfact and governance structures beg the question: given that there have been a number of opportunities to take advantage of the system, why have there not been a proliferation of adverse events? This work hypothesizes that the answer lies in the very concept that Nakamoto believed Bitcoin could overcome: trust. Throughout research on the topic of cryptocurrencies, trust, especially among developers and by other stakeholders upon developers and miners to satisfy the needs of system, has been a key theme. For example, the emergence of new lead developers was based on their reputational value, rather than any technical interface. Much as Williamson and March hypothesized, trust served as a mitigating factor that underscored sometimes ill-defined governance-based relationships within actors.
The ultimate conclusion of this analysis indicates that the governance of cryptocurrency reflects its theoretical promise: individuals' desire to innovate to increase their stake and power within any given system will always create the need for governance, regardless of the novelty of the technical interface that underlies it. The need for actors within cryptocurrency, especially miners and developer, to cooperate and collaborate across a joint

resource in the long term necessitates non-technical governance to ensure this innovation does not occur. Far from achieving the utopian promise of technical governance, cryptocurrency has endured growing pains resulting from the absence of these very systems. The technology alone is and will not be enough to sustain the wellbeing of cryptocurrency in the long term. This is evidenced not just by the conclusions of this paper, but by the actors within these cryptocurrencies themselves: as previously mentioned, Bitcoin developers have begun to develop a richly nuanced decision rights system since its fork, and lead developer Colvin is actively leading discussions about strengthening the premise and rules within Ethereum governance. As March theorized, the structure of governance within cryptocurrency is being bargained for by multiple stakeholder groups. In effect, this paper highlights that stakeholders of Bitcoin, Ethereum, and other cryptocurrencies should actively be thinking about the design and structure of their governance systems instead of attempting to avoid it entirely[68].

3.3.1 Blockchain technologies: a double governance

Blockchain-based organizations such as cryptocurrencies compete with traditional economic institutions by proposing alternative forms of organizational governance. Specifically, they upset the traditional principal–agent relationships by placing machines (i.e., the blockchain software program) at the core of organizational governance, and human actors (i.e., stakeholders) at the edges. Although humans are still involved in the creation, modification, and decision making about the code, now formal organizational rules and routines are written directly in the software program. In short, blockchain based governance in the context of cryptocurrencies calls for a revised understanding about power and control within the organizations. In the context of cryptocurrencies, not only is governance borderless, but also decentralized, albeit to various extents. Anyone can decide to "join" a public cryptocurrency organization, maintain, and update the open ledger based on "competitive bookkeeping" such as mining or other consensus mechanisms. Admittedly, decentralization distinguishes blockchain-based corporate governance from the traditional model based on hierarchies. It is important to note that cryptocurrency governance models can exist in different degrees of decentralization. Decentralization, on the one hand, creates value for cryptocurrencies as a peer-to-peer payment system that does not rely on centralized financial intermediaries such as banks or payment companies. On the other hand, decentralization can create excessive inefficiencies as governance decisions are made without centralized authorities, but through consensus mechanisms in a non-hierarchical fashion. Following the corporate governance literature, we distinguish between the internal and external governance features of cryptocurrencies. While the effectiveness of internal governance is typically rooted in the design of incentives,

[68] Nagarajan, M. (2018). An Analysis of Cryptocurrency Governance.

the effectiveness of external governance depends on the influence exerted by the community, the media, and the general public over the organization. Considering how cryptocurrencies are structured, we distinguish, internally, between the blockchain, the protocol, and the organizational levels, and externally between the community, media, and social levels. Here we identify three internal governance forms: owner control at the blockchain level, formal voting at the protocol level, and centralized funding at the organizational level. The blockchain level. At the blockchain level, miners (or validators in general), whose behavior is guided by the rules and incentives encoded in the cryptocurrency's software, constitute the key stakeholder group. On the one hand, miners/validators work by the software's rulebook and are incentivized accordingly. In this regard, miners/validators work like "employees" who are governed by predetermined incentive mechanisms. On the other hand, miners/ validators have the power to decide which transactions to accept into a block, as well as to agree or disagree on the "longest chain" that will constitute the trusted version of the distributed ledger that all users will follow going forward. However, there are different ways to tie transaction validation to cryptocurrency ownership. For instance, while a proof-of-work (PoW) miner does not have to own the cryptocurrency to mine, on proof-of-stake (PoS) blockchains, validators are incentivized in proportion to the amount of cryptocurrency tokens they hold. In sum, there are three governance design features at the blockchain level associated with more centralization: the use of PoS, the use of pre-mining, and the use of nomination.

The protocol level. Developers who specialize in programming blockchain applications constitute the key stakeholder at the protocol level as they are the people who "write the rulebook". For most cryptocurrencies including Bitcoin, developers work on a voluntary basis and are not hired or funded by any centralized organization. The code that they work on is typically open source, meaning that any developer can contribute to the code using online repositories such as Github.com (which acts as the Wikipedia of software development). Still, a small group of very dedicated "core" developers can be formed, and governance decisions may thus become more centralized. The organizational level. In theory, the formative ideology behind Bitcoin and many subsequent cryptocurrencies is rooted in the ideas of decentralized control over token distribution, network participation, and openness. However, there are still substantial differences in how cryptocurrencies are governed in practice. For example, unlike Bitcoin, Ripple has its network and tokens centrally managed by the Ripple company, a venture capital-backed start-up with offices based in five locations: San Francisco (headquarters), New York, London, Luxembourg, and Sydney. Under this more centralized model, management strategies not only are prevalent but necessary for the cryptocurrency-as-company to attract external funding and grow. The presence of such centralized funding reflects a more centralized form of governance. External governance mechanisms influence organizations less through formal mechanisms such as control over decision rights or ownership rights, than through informal social mechanisms such as social evaluations, reputation effects, informal voting, or public image. Arguably there is very little room for external forces to exert formal and direct influence over the blockchain, even through developers and

miners. Further, external actors attempting to make alterations to technical features can create controversy. In the following, we identify three specific external governance forms: community governance at the community level, negative publicity at the media level, and public interest at the social level. Community level. Many cryptocurrencies were created from the open-source Bitcoin software code, and follow the same open-source development model. Like many open-source software projects, initial participation is usually driven by the need for software-related improvements, but later evolves with developers becoming hobbyists. However, compared with open-source software communities, cryptocurrency communities generally consist of a much more diverse base of stakeholders, including: developers, miners, start-ups, enthusiasts, and users. Community governance involves forum discussions and sometimes informal online voting over decisions. The most used forums for cryptocurrency discussions include cryptocurrencies' official forums, specific cryptocurrency sub-groups within forums such as bitcointalk.org, Reddit.com, and social media such as Facebook and Twitter. These external stakeholders take on an "active and possibly democratic role in the management and operation of the organization". Media level. Recent developments in the corporate governance literature have treated media as an important source of external governance. Different from controlling through ownership and decision rights, the media can influence key stakeholders of an organization by serving as an information intermediary that plays a governance role through informing, monitoring, and reputation effects, In particular, scholars have demonstrated that negative publicity conveyed in the media is especially effective in influencing organizations. Social level. The third source of external corporate governance mechanism is rooted in public interest from the broader society. Public interest pertains to aggregated search activities motivated by curiosity, attempts to learn, or understand the technology, and cryptocurrency-related affairs. Arguably, cryptocurrencies that receive greater public interest are also subject to more decentralized monitoring and scrutiny regardless of the nature of search and intention[69].

The blockchain economy demands a reassessment of established notions of governance. However, how exactly governance will change in the emerging blockchain economy is still little understood. Nevertheless, the promise of the blockchain economy is dependent on the implementation of effective governance mechanisms, which are, in turn, dependent on a thorough understanding of the phenomenon. Finally, the role of incentives in the blockchain economy should be further explored. Among other things, research is needed to gain a better understanding of how incentives relate to consensus in the blockchain economy[70].

[69] Hsieh, Y., Vergne, J., & Wang, S. (2017). The internal and external governance of blockchain-based organizations: Evidence from cryptocurrencies. (pp. 48-68)https://doi.org/10.4324/9781315211909

[70] Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems, 19*(10), 1.

3.4 Crypto-regulation: the position of international organizations and possible future development

Cryptocurrencies and blockchain technologies pose difficult challenges for policy makers. There is no regulatory framework for transfers made with cryptocurrencies or smart contracts. Transfers occur outside anti-money-laundering compliance programs, and smart contracts are not subject to consumer protection laws or financial oversight. Tax codes do not fully cover the new markets if cryptocurrencies are not recognized in the law as payment systems but are instead viewed as commodities. It is difficult to determine the geographic location of the value added created by cryptocurrency mining. Tax legislation therefore has to be adjusted to incorporate these new activities into direct and indirect tax systems. Another ambiguity for policy makers is whether these new activities should be supported or constrained. Should they be encouraged because of positive externalities and first-mover benefits? Or should they be constrained because they crowd out investments with greater social return? Another pertinent question for policy makers is whether and how they can use these technologies to improve their own services. An undesirable side effect of the cryptocurrencies is the outsized use of electricity in mining. If mining companies pay a lower electricity price than the marginal cost of supplying more electricity, governments should consider raising tariffs or at least calculating the implicit subsidy. The sharp increase in electricity demand might be an opportunity to develop an electricity market with intra-day price fluctuations, so that price differentiation reflects actual costs. Uncertainty about future electricity demand for cryptocurrency mining warrants a rethinking of contingent liabilities of governments where additional power plants are built by public-private partnerships. Guarantees related to future demand for electricity used in cryptocurrency mining are riskier than for other electricity demand. Ultimately, financial oversight will cover cryptocurrencies and smart contracts. This process will be a gradual one of trial and error, and it will depend on the direction in which blockchain applications develop. First steps have already been taken, in the United States (where bitcoin can be traded on futures markets), in Switzerland (where regulation of ICOs was proposed), and in the Netherlands (where guidance was provided about the tax treatment of cryptocurrency holdings). Oversight to prevent money laundering, tax evasion, pump-and-dump schemes, and illicit cross-border transfers focuses on transactions in which cryptocurrencies are exchanged for legal tender. The ultimate goal of all these efforts is to create a level playing field, so that blockchain application can be integrated into existing markets. The long-term outcome could be that supervision becomes much more effective because the transparency of the blockchain could provide supervisors and courts with access to real-time information. The many experiments and brainstorms by governments and central banks throughout the region are inspiring. Just as blockchain opportunities put competitive pressure on private financial sectors, they also trigger creative thinking in governments. It is important that these experiments not consider current blockchain designs as the full universe of possibilities. Even if decentralized maintenance of

digital government data can have major advantages, a permissioned system seems much more appropriate and efficient for governments than the original system that maintains the blockchain for cryptocurrencies[71].

Starting with bitcoin, there has been a remarkable proliferation of digital currencies, or cryptocurrencies, offering an alternative to the traditional, bank-based payments system which has underpinned the role of bank liabilities as money. But how far can digital currencies be regarded as money? Any asset, to act as money, must have the characteristics to allow it to perform the three functions of means of payment, unit of account and store of value. As Yermack (2013) argues, bitcoin (the leading digital currency) fails on all three counts. First, empirically, digital money is used more for speculative transactions than for purchases of goods and services, and so does not seem to function well as a means of payment. This is not surprising since supply is limited, transactions are cumbersome (encouraging the emergence of break-away currencies like bitcoin cash), and, unlike payment by credit card, funds must be available in advance of purchase. Bitcoin also falls short as a unit of account because of its highly-variable value, the range of prices quoted in different sites, and its high denomination relative to many retail transactions. Third, bitcoin does not act as a store of value in the sense of having stable value. As long as bitcoin holders are confident its value will not fall, it seems to be an excellent store of value, but the volatility of its price makes it more suitable as a speculative investment than an asset to hold when expectations of returns on alternative assets are highly uncertain[72].

Virtual currencies (VCs) are a relatively new invention and have only recently begun to attract the attention of financial regulators. Individual countries have different attitudes towards VCs. In most countries, especially in major jurisdictions, authorities have adopted the "wait and see" attitude, while closely monitoring developments in VC markets. Several financial authorities have issued informal warnings to the general public, advising of the dangers of involvement in VCs. One may expect that, with some time lag required to learn and comprehend the new phenomenon and its potential economic and legal consequences, all major jurisdictions will attempt to regulate the use of VCs, and perhaps, as in case of other financial regulations, there will be some effort to harmonise them. Without the risk of guessing the unpredictable future, one cannot expect, however, that VCs will be accepted as the official means of payment or unit of account soon. That is, paying taxes, public sector salaries, pensions, and other social benefits, or making public transfers, among others, in VCs appears a highly unlikely scenario. The same applies to the possibility of using VCs as a unit of account in official financial, tax, or statistical reporting. Furthermore, financial supervisory authorities can increasingly consider VCs as risky financial assets subject to strict precautionary prudential regulations or even legal bans

[71] World Bank (2018), *Cryptocurrencies and Blockchain*, World Bank Europe and Central Asia Economic Update, Office of the Chief Economist, May, Washington.

[72]Dow, S. (2019). Monetary reform, central banks, and digital currencies. *International Journal of Political Economy, 48*(2), 153-173. https://doi.org/10.1080/08911916.2019.1624317

which may limit their use by licensed financial institutions, and therefore, the general public. The same concerns anti-money laundering and anti-terrorist finance legislation. Investment in VCs may become increasingly subject to income or transaction taxes, a phenomenon already observed in several countries, which can limit the interest of potential investors. However, one cannot have the illusion that even the strictest regulations and bans can entirely eliminate the use of VCs as a means of payment in cases of private transactions (especially cross-border ones) or as a store of value (a financial asset in which some economic agents will be interested to invest). The cross-border harmonisation of financial and tax regulations and the cooperation of financial regulatory authorities is never perfect, which will leave room for cross-border arbitrage. Furthermore, as history teaches us, financial regulations always lag behind financial innovations, while VCs are a new invention with great potential for further technological development. Therefore, financial supervisory or monetary authorities will not be able to regulate in advance all new potential variants of VCs which may appear. For all of the above-mentioned reasons, one must be prepared that VCs will remain a stable component of the global monetary and financial architecture for several years to come[73].

The advent and speed of financial innovations brought about initially by the Internet that serves as a basis for the transformation of global payment systems inevitably has raised significant concerns among law enforcement agencies about criminal activity. Among the issues are concerns voiced by national central banks about the incorporation of new currencies into the global financial network and governmental apprehensions in their endeavor to protect their citizens from harmful investments. The Bank for International Settlements (BIS), through its Committee on Payments and Market Infrastructures, issued a report on digital currencies in November 2015. In the report, BIS set forth the supply-side factors that may influence the currencies' future development which primarily are fragmentation due to the numerous digital currencies in circulation; scalability and efficiency, which at the time of this report, was smaller than traditional payment systems; pseudonymity (not anonymity) inasmuch as the distributed ledger is usually publicly available; technical and security concerns by malicious actors using falsified ledgers; and business model sustainability that will be difficult to achieve. It also noted the demand-side issues of security, cost, usability, volatility, risk of loss, irrevocability, processing speed, cross-border reach, data privacy, and marketing and reputational effects. The regulatory issue BIS addresses is the degree of regulation that should occur both on a global and national level. BIS also addressed the implications of virtual currencies for central banks and their role in acclimating to virtual currencies. BIS' emphasis is on consumer protection and the basis for its value predicated on the user's perception of value. With the decentralized nature of virtual currencies, it will be difficult for central banks to anticipate possible disruptions. There are legal risks due to the lack of a legal structure to govern their

[73] Dabrowski, M., & Janikowski, L. (2018). Virtual currencies and central banks monetary policy: challenges ahead. *Monetary Dialogue. Policy Department for Economic, Scientific and Quality of Life Policies. European Parliament. Brussels*.

use. There are implications for financial stability and monetary policy owing to their impact on retail payment systems, liquidity for central banks, and the degree of interconnection between users of traditional and non-traditional currencies. A future course of action may include banks' own investigations of the distributed ledgers in payment systems. The European Central Bank (ECB), as early as October, 2012, was concerned about virtual currencies shortly after their issuance. It referred to them as "virtual currency schemes," because of the two aspects of resembling money and possessing their own retail payment systems. After reciting the characteristics of the currencies, it noted the business reasons for their creation and growth, namely, for virtual community users to participate in them; to generate revenue for their owners; to have control over them in accordance with their business model and strategy; and to compete with traditional currencies such as the euro and the dollar. In a later report in 2015, the ECB noted the dramatic increase in the number of decentralized virtual currencies and the increased dangers to the payment system and, perhaps, more importantly, to the users who are exposed to risks of exchange rate, volatility, counterparty relating to the anonymity of the payee, investment fraud, and other risks. It expressed concern over the lack of co-ordinated governmental efforts from national authorities to mitigate these risks which range from warnings, statements, and clarification of the legal status of the currencies, to licensing, and supervision of their activities. It thus recommended a co-ordinated response by the legislative, regulatory, and supervisory frameworks to the various schemes discussed in its earlier report. The UN expressed its concern about virtual currency in the context of terrorism. In addition to resolutions condemning terrorism, it has commenced a joint project between the UN Counter-Terrorism Committee Executive Directorate and the Swiss non-governmental organization ICT4Peace entitled "Tech against Terrorism." The public-private endeavor is directed towards the prevention of the spread of terrorism through the use of the Internet. Included is the restraint of use of virtual currencies by the groups[74].

It is useful in this analysis to mention the role of the International Monetary Fund, a specialised agency of the United Nations, whose primary objective is to ensure the stability of the international monetary system. As Bitcoin continues to grow in popularity and value, it poses an increasingly serious threat to the stability of the foreign currency exchange market and, by extension, international commerce. Recall that the IMF was created to tackle two global economic problems: (1) the artificial devaluation of one's currency to gain an economic advantage;" and (2) unstable exchange rates between various currencies. Bitcoin cannot trigger the first concern because the algorithm that supports it prohibits users from artificially manipulating its value. Bitcoin does, however, have the potential to create severe and possibly irreversible fluctuations in the foreign currency exchange market. Specifically, Bitcoin poses a liability to the IMF and its member nations in the event it is used in what is referred to as a "speculative attack" on another currency. Finding a way to regulate Bitcoin is critical in light of its potential destabilizing effects on the foreign currency exchange market. The

[74] Girasa, R. (2018). *Regulation of cryptocurrencies and blockchain technologies: national and international perspectives*. Springer.

IMF is particularly well-situated to solve this problem for two reasons. First, the IMF is an institution specifically designed to help stabilize the global economic system via the foreign currency exchange market, as explained in Section III. Second, regulating Bitcoin falls squarely within the IMF's goals, as outlined by Article 1 of the Articles of Agreement. In both of these respects, the IMF is able to coordinate a global response to the threat posed by Bitcoin in a way no other institution can. There are, however, challenges that must be overcome. The most obvious obstacle to regulating the impact of Bitcoins on the foreign currency exchange market via the IMF is one of enforcement. Article VII of the Articles of Agreement allows the IMF to replenish its holding of a member nation's currency. It also allows the IMF to restrict the flow of a currency it deems to be scarce and to apportion its allocation accordingly. Both are vital tools for countering a speculative attack. Neither of these tools, however, is available to the IMF in the event of a speculative attack by Bitcoin users. The IMF draws its power from the obligations it imposes via the Articles of Agreement. Those obligations only bind members of the IMF (that is, signatories of the Articles of Agreement). Consequently, Article VH only authorizes the IMF to collect currency from member nations. Membership, however, is only open to nation-states. As they are now, the Articles of Agreement do not permit the IMF to exercise direct control over the use of Bitcoins. There are, however, two ways to incorporate Bitcoin into the IMF's regime. The first option is to grant the IMF indirect control over Bitcoin by expanding the interpretation of an already-existing provision of the IMF. This approach requires the least amount of change and leaves the overall IMF framework mostly intact. The second option is to grant the IMF more direct control over Bitcoin by granting it and other digital currencies quasi membership status. This more radical approach would require an amendment of the Articles of Agreement and would fundamentally alter the existing framework's conception of a non-state actor's role in the IMF[75].

The regulatory landscape surrounding blockchain technology would significantly benefit from an international convention determining which investor and consumer protection regimes are applicable, and at which venues victims of fraud or misrepresentation may sue initiators of token sales. The analytical preconditions for such a convention are arguably in place. Therefore, the international landscape concerning token sales, and blockchain organizations more generally, is reminiscent of the debates surrounding the law applicable to content uploaded on the Internet. Again, there is a twofold danger: first, that overlapping regulatory regimes excessively burden developers (regulatory overkill); and, second, that contradictory content of the regimes effectively undermines investor and consumer protection (regulatory perplexity). But as sensible as the case for international regulation may appear prima facie, it is less clear how to incentivize the ubiquitous ratification of a “Crypto-Security Convention”. This is because there is strong holdout potential especially for small countries like Panama or Gibraltar, similar to what we have been seeing in the field of international tax

[75] Plassaras, N. A. (2013). Regulating digital currencies: bringing Bitcoin within the reach of IMF. *Chi. J. Int'l L., 14*, 377.

harmonization. One can conceive of solutions to that problem. The strategic objective would have to be that the benefits of ratification, i. e. becoming a member of an integrated legal area for blockchain regulation, have to exceed the idiosyncratic benefits of non-ratification. Generally speaking, a convention would have to be accompanied by unilateral prohibitive regulation, effectively shutting down the national market for foreign crypto-security issuers not in compliance with such convention. Hence, a "Crypto-Security Convention" would exert thorough and resourceful preparation. The Hague Conference of International Law, UNCITRAL and UNIDORIT, conceivably even the International Law Commission or the Hague Academy of International Law, seem perfectly able to heed this call and start working on draft articles and an intelligent implementation strategy. Furthermore, in 2018, several international initiatives have been launched by financial standard-setting bodies, such as the Financial Stability Board, the International Organization of Securities Commissions, and the Basel Committee for Banking Supervision, to monitor, evaluate and support ICOs; they are being actively discussed at the G20 level, too. International ICO standards could indeed pave the way for an international convention. Eventually, crypto-securities may also provide a blueprint for the development of an international convention on blockchain organizations more generally – be they cryptocurrencies, token-based decentralized applications, or else[76].

[76] Hacker, P., & Thomale, C. (2018). Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law. *European Company and Financial Law Review*, *15*(4), 645-696.

Chapter 4

The geopolitics of cryptocurrencies

4.1 What is the geopolitical influence of cryptocurrencies?

The development and evolution that the cryptocurrency market has undergone over the past decade has not left corporations, companies, nation states and international organisations indifferent. The last chapter explored full the positions regarding the emergence of digital currencies and therefore the positions that a number of the big international financial institutions have taken in regard to this growth. However, of particular importance is that the approach that some states have appropriated the years, either by trying to use the chance that has emerged, or by setting up place measures to scale back the employment of cryptocurrencies the maximum amount as possible, or finally by proposing the creation of their own national cryptocurrency. All this obviously results in strong repercussions within the geopolitical sphere. As mentioned above, some cryptocurrencies, like Bitcoin, are available in limited numbers (by statute, the quantity of bitcoins produced cannot exceed 21 million). The consequence of this can be mining, which has become increasingly competitive and complex over the years. For this reason, while within the early stages of development mining was done by individuals attracted by the profitability of mining, today it's mostly companies with video cards and processors linked to the network. Mining is after all linked to electricity, the number of processors and video cards, the computing power used and, above all, the country during which one is found. Indeed, the mining of a Bitcoin varies from country to country, betting on the worth of electricity. It takes 20 Gigawatts to mine one Bitcoin in 10 minutes. Regarding the value of electricity, Venezuela is one in all the most cost-effective countries (530$ per month) and Asian country is one in every of the foremost expensive (26000$ per month). However, there are some countries that are highly strategic for mining. In Iceland, for instance, by virtue of its heat, a knowledge centre with quite 30,000 computers has been established (Genesis Ethereum mine). The country is perfect because of its cold climate and where most energy comes from renewable sources, with very low and advantageous prices. On the opposite hand, it should even be noted that about 90% of the energy expenditure is generated by cryptocurrency mining. Until 2017, 80% of mining transpire in China, until the government decided to maneuver to do to significantly limit the phenomenon, as we'll specify later. It seems quite clear that the rise in demand for cryptocurrencies and their exchange, which, as is well-known, doesn't require financial intermediaries, takes place in places where the financial condition persists and where conditions of strong economic instability like inflation are present. In Sub-Saharan Africa, a complete of quite $50 billion has been transferred within the sort of cryptocurrencies, helping to save lots of some $2 billion in transfer fees. In other states, however, like Nepal, Algeria and Bolivia, holding Bitcoin may also cause arrest

and countries like India are preparing countermeasures, like banning cryptocurrencies so as to issue a politician one at government level. the identical applies to China and Russia, with the proposal of a digital Yuan and Ruble, with the aim of moving far from the dollar monopoly and strengthening their influence. China is that the incumbent, trying to dethrone the US because the world's economic superpower. an enormous a part of this is often destroying the world's dependence on the U.S. dollar. In other words, China doesn't want the USD to be the reserve world currency. Does this mean they require the Yuan to be the reserve currency? It seems that way. China contains a lot of success selling its products, but not many countries want to carry their currency, the Yuan. Currently, The Yuan accounts for less than 2% of world reserves, though this is often forecast to extend. Meanwhile, the US dollar accounts for 60% of world reserves, though this number has been decreasing within the last 10 years. One way of staring at China's intentions is that anything that helps displace the US dollar, is in China's interests. This is often where Bitcoin comes into the equation. Bitcoin, and a few other cryptocurrencies, are challenging paper money. However, the one that has the foremost to lose, is that the dollar, since it's the reserve currency. So, is Bitcoin controlled by the Chinese? Some estimates say that around 75% of all Bitcoin is mined in China. These Chinese miners, therefore, can exercise plenty of power thanks to their immense hash rate. But does that mean they'll control the network? Technically yes, but what would happen if they did? Ultimately, if people saw this as an illegitimate attack, Bitcoin would hand over to a replacement chain, nodes would switch then would miners. Cryptocurrency, like all other variety of money, needs social consensus to figure. Therefore, the opposite theory we could extrapolate, is that, quite contrarily, China is frightened of Bitcoin, since it'd wish to control and keep tabs on monetary transactions, and Bitcoin doesn't allow this. China has many reasons to be petrified of Bitcoin, but it might be a necessary evil if it wants to dethrone the US dollar regime. However, the foremost recent evidence doesn't suggest that Bitcoin is displacing the US dollar. Where Bitcoin has an impression though, is in displacing volatile currencies, just like the Turkish lira or the Argentinian Peso. Bitcoin is appearing as a sound alternative to those currencies, but it's still second to the dollar[77].

4.2 How the attitude of the world's governments has changed in relation to the growth of cryptocurrencies

The governments of the G7 are cognizant of the advantages of digital financial technology, but also are hugely concerned about the general public policy and geopolitical threats from this potentially disruptive innovation, especially from so-called 'global stablecoins' (GSCs) operated by loosely regulated, non-financial technology giants, but denominated in national currencies. A recent G7 report warns such innovations raise serious

[77] The Value Trend (2021), "The Geopolitics of Bitcoin", Seeking Alpha, https://seekingalpha.com/article/4428654-the-geopolitics-of-bitcoin-btc , (viewed on 03/09/21)

questions about a variety of public policy issues, including 'challenges to fair competition, financial stability, monetary policy and, within the extreme, the international monetary system'. G7 ministers and governors have stated quite explicitly that no global stablecoins should begin operation until regulatory and oversight issues are resolved. These governments have recognised the necessity for international cooperation on how private digital currencies should be regulated, not least because the choice – a world free-for-all – may be chaotic and dangerous. However, they also see that well-regulated digital currencies can provide significant public benefits in greater efficiency and lower costs for both domestic and, particularly, international payments systems, and help ensure financial services reach the many legion people – especially in developing countries – without bank accounts. The expansion of huge tech firms into global finance remains in its infancy. But, as these giants expand and banks themselves widen their digital footprints, financial technology will reshape not just the commercial but also the geopolitical sphere. Former UK national security adviser Sir Mark Lyall Grant recently warned of the Chinese financial threat from a digital RMB (renminbi), writing that the introduction of a 'digital yuan' would give China the 'ability to bypass the world's traditional banking systems and so challenge the dollar's pre-eminent position'. In 2019, then Bank of England governor Mark Carney spoke of the 'destabilizing asymmetry' of the international touchstone, lamenting the 'domineering influence' of the dollar and indicating a full of life discussion is well underway about the potential impact of digital currencies on global politics. Carney identified the RMB because the presumably candidate to affix the dollar as a 'true reserve currency', noting the RMB is making significant progress as a medium of exchange particularly in trade and finance. He said his view was that technology could play a task in facilitating the emergence of a brand-new global reserve currency - and a digital RMB can be one step therein process. The widespread introduction of digital currencies has the potential to remodel the planet economic system. In January 2020, a gaggle of advanced economy central banks – from Canada, the UK, Japan, Sweden, Switzerland, and therefore the European financial organization – announced they were working together on financial organisation digital currencies under the auspices of the Bank for International Settlements (BIS). The US Fed Board has since joined too but China, despite launching trials of a domestic digital RMB, appears to not be a part of the group. Certainly, the looming geopolitical challenge from China could be a motivation for others – especially G7 economies – to cooperate. But cooperative agreements among these central banks could also play a pivotal role in shaping not just international standards for sovereign digital currencies, but also for the regulation and supervision of a more deeply digitized global economic system. and also, the chances of this advanced economy group of central banks working together are enhanced by the arrival of President Joe Biden within the White House. As China takes forward its own plans for a digital currency with a financial set-up boasting a number of the biggest 'fintech' firms within the world, this can be a threat to US leadership in digital finance and also the dollar's role at the centre of the international standard. Given the globally-integrated nature of finance today, the US would protect its own interests best by cooperating with other like-minded governments

to shape the design of digital finance together, instead of concentrate on a dogged defence of the dollar's traditional position[78].

As widely analysed, approaches differ both at the national level and in international dialogue forums. In the complex universe revolving around cryptocurrencies and their use, I've got chosen to appear at three national cases and also the different policies that are put in situ.

4.2.1 China's case

As with most other nations within the world, China chose to adopt a "wait and see" approach when it came to regulating Bitcoin. aside from a ban by the govt. that prevented banks and traditional domestic exchanges from investing/trading Bitcoin in 2013, there was no strict regulation implemented until 2016. This allowed Bitcoin to flourish in China in its early years. In 2011 the primary Chinese Bitcoin exchange, BTCChina, was launched. It had been not until 2013 that Bitcoin really began to gain traction in China. Up until now the sole real headlines involving Bitcoin were negative, associated with skepticism, scams, and its links to the black market. This changed in April 2013, when a Chinese charity called the One Foundation announced that it absolutely was accepting Bitcoin (the only crypto within the world at this time). After an earthquake hit China that year the charity was received 230 BTC, worth around $30,000 at the time, and 1% of all fundraised for relief. State media released positive reports and likened Bitcoin to other digital centralized currencies like Q Coin. In May 2013, the Huobi crypto exchange was founded, as was Bitmain, a corporation who in 2018 was the world's largest designer of computer chips specifically for Bitcoin mining. The Chinese state computer programme, Baidu, began accepting Bitcoin. Taobao, the world's largest e-commerce site followed their lead, and demand for Bitcoin soared. BTTChina became the biggest crypto exchange within the world by volume, surpassing the now infamous Mt. Gox. the rise in interest for Bitcoin in China pushed the value from $50 to new record highs, seeing an 800% increase in precisely two months. The national program and also the biggest e-commerce website accepting Bitcoin as payment perceived to have the crypto on a path to legitimate and widespread adoption. But in early December 2013, the Chinese financial organization, together with five other government ministries, released an announcement saying that Bitcoin couldn't be used for products and services, which financial institutions couldn't buy or sell them. it had been declared illegal tender. Baidu and Taobao removed their Bitcoin payment options, and also the next day Bitcoin dropped 20% in value[79].

---

[78] Fleming. S., Pickford, S. (2021), "Digital currencies: Economic and geopolitical challenges", Chatham House, https://www.chathamhouse.org/2021/01/digital-currencies-economic-and-geopolitical-challenges , (viewed on 03/09/21)

[79] Jones E. (2020), "A Quick History of Cryptocurrency in China", CryptoVantage, Internet: https://www.cryptovantage.com/guides/history-of-crypto-in-china/ (viewed on 04/09/21)

Bitcoin's rise in China began in 2013. within the following years, Chinese exchanges grew to dominate the worldwide exchange market, as shown by the relative share of Bitcoin exchange transactions executed in Chinese Yuan (CNY) versus other currencies. Mining pools managed by individuals in China have constituted over 1/2 the full network hash power since 2015 and currently more hash power is found in China than in the other country. Through this point, China's official position on Bitcoin remained ambiguous and regulators proved unwilling to institute tight controls despite expressing concerns over criminal activity, subversion of capital controls, and speculative risk. At the time of writing, 74% of the hash power on the Bitcoin network is in Chinese-managed mining pools. Pool miners can't be directly controlled by China, but the managers are located within China and per se are subject to Chinese authorities. Because managers are chargeable for assigning mining jobs and propagating completed blocks, they control the inputs and outputs of their miners, allowing Chinese authorities indirect control over that hash power. China has more direct control over the hash power physically located in China. this can be a major share of the worldwide hash rate – quite controlled by the other single country – but the precise quantity is unknown[80].

Table 4.1 – Nationality of mining pools and their share of hash rate between May 1, 2015 and June 30, 2016

Mining pool	**Located in China**	**Estimated share of network hash rate**
F2Pool	Yes	22.17
AntPool	Yes	21.54
BTCC	Yes	12.79
BitFury	No	12.39
BW Pool	Yes	7.84
KnCMiner	No	4.89
SlushPool	No	4.72
21 Inc.	No	2.27

Table of own production; Source: Kaiser, B., Jurado, M., & Ledger, A. (2018). The looming threat of China: An analysis of Chinese influence on Bitcoin. *arXiv preprint arXiv:1810.02466*.

The Law on People's Bank of China designates the People's Bank of China ("PBoC") the only real authority to issue currency and manage the currency circulation. Article 20 forbids any unit or person apart from the PBoC from printing or issuing token tickets that might replace renminbi. Article 16 emphasizes that renminbi

[80] Kaiser, B., Jurado, M., & Ledger, A. (2018). The looming threat of China: An analysis of Chinese influence on Bitcoin. *arXiv preprint arXiv:1810.02466*.

is that the only "legally mandatory currency" that not a soul or unit can refuse payment in renminbi specially to repay either public or private debt. Additionally, the State Administration of interchange ("SAFE") has imposed a $50,000 annual cap on total amount of exchange that a personal may acquire. To enforce these limitations, the SAFE appoints exchange banks to look at, validate, and track each transaction. Both the PBoC and also the SAFE explicitly forbid individuals from directly investing in foreign capital markets without approval from local interchange departments. Violation of such rules may lead to criminal liability. In December 2013, PoBC and 4 other ministries together released an announcement regarding bitcoin and other virtual currencies ("the 2013 Announcement"), declaring that bitcoin isn't a currency, but it might be treated as a "virtual asset or digital commodity." The 2013 Announcement explicitly disallowed financial institutions and payment companies from engaging in bitcoin-related businesses. While the 2013 Announcement prohibited bitcoin as a payment instrument for goods and services, the investing public was absolved to buy and sell "online commodities," implying that exchanges among bitcoin and cryptocurrencies weren't prohibited. Meanwhile, the 2013 Announcement warned the general public about the anonymous nature of bitcoin and declared it a "speculative asset." The Chinese government also claimed to extend oversight of bitcoin related websites and reduce concealing risks related to bitcoin." Although the 2013 Announcement only claimed to broadly regulate cryptocurrency "from an awfully macro-level, not [to] blindly try and regulate a market in its infancy,"' the value of bitcoin still dropped by about 50% afterwards. Twelve months before the crackdown, China dominated the bitcoin exchanges market, accounting for over 90% of trade volume. The heyday failed to last. In September of 2017, the PBoC and five other ministries announced that financings using cryptocurrency, like ICOs, are "in nature unauthorized illegal public financing, and [are] suspected of [being involved] within the illegal sale of coins, illegal issuance of securities, illegal fundraising, financial fraud, pyramid sale and other illegal and criminal activities." This 2017 Announcement also restated the government's position within the 2013 Announcement that bitcoin, ether, and other cryptocurrencies don't function as money because they need no "legal tender status" and their use "is not legally mandatory." Although the 2017 Announcement categorized bitcoin as "coin substitution" or "virtual currency" without addressing the cryptographic aspect of the currency, it explicitly banned any exchange between folding money and "coin substitution," and also the circulation of such "coin substitution." The Announcement also explicitly prohibited any offering or financing activities of cryptocurrency, and required organizations or individuals that "completed" the crypto-financing to terminate the investment contracts and "dispose of risks in an appropriate manner." The 2017 Announcement also delegitimized "the so-called coin financing exchange platform[s]." It not only restated the position within the 2013 Announcement, but also further limited financial institutions from trading, pricing, or acting as office for crypto exchanges. Nevertheless, the 2017 Announcement failed to mention any pecuniary or criminal liabilities for any regulatory noncompliance, especially against entities that aren't registered as "financial institutions." The Announcement also didn't explicitly forbid exchanges or

transactions among cryptocurrencies, nor did it ban mining or try and place any blockchain development under surveillance[81].

More recently, China has increased restrictions on the prohibition of financial institutions and payment companies from providing cryptocurrency-related services. Trading in cryptocurrencies has been illegal in China since 2019, to prevent money laundering. On 18 May, three government organisations, the National Internet Finance Association, the China Banking Association, and the China Payments Association broke the news. They said that consumers would have no protection if they incur losses related to cryptocurrency transactions. They added that the recent price changes in cryptocurrencies seriously violate the safety of investors' assets and damage the normal economic and financial order. As in the previous 2017 ban, it is expected that banks and online payment services will not offer services related to cryptocurrencies, including account opening, registration, trading, and insurance. However, there is some news. The People's Bank of China has clarified that institutions must not accept cryptocurrencies or use them as a means of payment. Nor will it be possible to carry out exchange services between cryptocurrencies and yuan or foreign currencies. In addition, the institutions are prohibited from providing savings services, trusts, or dispensing financial products related to cryptocurrencies. And cryptocurrencies may not be used as investment targets for fund or trust products. Beijing, rather than turning to cryptocurrencies in terms of financial innovation, is turning to the digital yuan. This is a way for the People's Bank of China to digitise coins and banknotes that are in circulation. Already the Chinese market is very advanced in terms of cashless payments. The digital yuan, which is technically referred to as digital currency electronic payment (CBDC), would speed up this process, which is already underway. Fan Yifei, executive of the People's Bank of China, said there is a pressing need to digitise paper money, as it is very expensive to produce and store. The distribution of the digital yuan is done through a two-tier system: the People's Bank of China distributes the digital yuan to commercial banks, which in turn distribute it to consumers. Beijing has already distributed millions of dollars in digital yuan in the cities of Shenzhen, Chengdu and Suzhou through lotteries held by local governments[82].

Finally, we come to the considerable changes and upheavals that took place this summer. Due to the Chinese government's increasing crackdown, many bitcoin miners have shut down their operations in China in recent weeks. According to several industry media reports, most of them are moving abroad, to places where electricity is cheap and the law is more favourable to them, such as Texas, in the United States, and Kazakhstan. The current size of the phenomenon - which has been given the name "great mining migration" -

[81] Xie, R. (2019). Why china had to ban cryptocurrency but the u.s. did not: comparative analysis of regulations on crypto-markets between the u.s. and china. *Washington University Global Studies Law Review, 18(2),* 457-492.

[82] Betro N. (2021), “Pechino tra criptovalute e yuan digitale”, Il Caffè Geopolitico, Internet: https://ilcaffegeopolitico.net/525510/pechino-tra-criptovalute-e-yuan-digitale (viewed on 30/07/2021).

is still unclear, but according to the Global Times, an English-language tabloid owned by the Chinese Communist Party, 90 per cent of the industry's capacity in the country (the so-called "mining farms") has already been stopped. Another proof that the number of miners in China is decreasing is the drop in the price of graphics cards, components used among other things in mining computers to make them faster: as reported by the South China Morning Post, on the Chinese e-commerce platform Tmall, the price of an advanced Asus RTX3060 graphics card dropped from 13,499 yuan (1,755 euros) to 4,699 yuan (611 euros) between May and June. Contributing to this drop is the fact that many Chinese are reselling their used equipment, which has even led China's largest cryptocurrency mining computer manufacturer, Bitmain, to suspend the sale of its machines so as not to lose out due to low prices. In Xinjiang (a remote province bordering Kazakhstan), where 36 per cent of the world's Bitcoin network computing power was concentrated in April, local authorities on 9 June imposed the closure of mining activities in the Zhundong Economic Technological Development Park, an area of 15,500 square kilometres that is home to several coal-fired power plants and some of the country's largest bitcoin mining facilities, which harness energy directly on site. In Sichuan, which in April was home to about 10 per cent of the world's computing power, the authorities ordered all mining activities to be shut down on 18 June, while a few days earlier in Yunnan, where about 5 per cent of the total hash rate comes from, the provincial government ordered the closure of mining activities that bypassed the state power grid by entering into supply agreements directly with the power plants. Newspapers have attributed this crackdown to several factors: China's desire to reduce its carbon footprint, to prevent the risks to the financial system from speculation on cryptocurrencies (as officially stated by Vice Premier Liu He), and to facilitate the adoption of its own digital currency, the DCEP or digital yuan. However, the specialist website CoinDesk pointed out that these are not plausible reasons. If the aim was to reduce emissions, the measures should have affected only miners in provinces where energy is produced mainly by burning hydrocarbons, such as Inner Mongolia and Xinjiang. However, as we have said, the authorities are also halting mining operations in provinces such as Sichuan and Yunnan, where energy is mainly hydroelectric. As for the risks of trading and the competition that bitcoin would pose to the digital yuan, these are issues that do not depend on where the miners are located. Some have speculated that the ban is aimed at stopping capital flows out of the country. Mining does indeed involve income in bitcoins, which can easily be transferred outside of China, as opposed to the Chinese currency. More likely, however, according to CoinDesk, is that the miners are an obstacle to China's attempt to rebalance its power grid. The problem with China's power grid is that several remote and sparsely populated provinces, such as Xinjiang, Inner Mongolia, Sichuan, and Yunnan, are rich in energy sources and have long produced a lot of cheap electricity, much of which was not used simply because there was not enough local demand and it was difficult to transport it, while the coastal regions, where the big cities are located, have long suffered from electricity shortages. In order to transport electricity from where there was unused supply to where there was unmet demand, an ultra-high-voltage power grid was needed, capable of travelling thousands of kilometres. The government started installing it in 2010 and in the last five years the balance between supply

and demand on the grid has improved a lot. According to CoinDesk, as long as the miners used the excess energy produced in remote regions, it was not a problem. But now that this energy can be used for other purposes, both industrial and commercial, mining competes with these different uses that contribute to the country's economic recovery. Since electricity is the main variable cost for miners, it is clear that they will move to places where electricity is cheap. According to CNBC, two likely destinations are Texas and Kazakhstan. The migration of miners could have important effects on the Bitcoin network: in the short term, the drop in the hash rate will mean that the problem to be solved to verify a block will become easier, making mining more profitable for the same price of bitcoin (fewer attempts and therefore less electricity will be needed). This is likely to attract new miners, driving up the hash rate in the medium term as Chinese miners resume operations where they have relocated. But the most important effect could be in the medium to long term: if Chinese miners find a place in different countries, the network will be much more decentralised than it has been so far and therefore much less subject to the laws of a single state. This would make the price of bitcoin less susceptible to news of industry regulation in a single country (as it has been so far with China), and perhaps therefore less volatile[83].

4.2.2 Venezuela's case

As already mentioned, the increase of different currencies occurs in those geographical locations where the crisis continues and where people are trying to find safe havens that don't seem to be subject to hyperinflation. within the case of the Bolivarian Republic of Venezuela, however, to lift the country out of years of severe depression and also the devaluation of its currency, the Venezuelan bolivar, it absolutely was the govt itself that announced the birth of a replacement state-owned cryptocurrency: the Petro. It's backed by the country's mineral and oil reserves. The Petro could be a suggestion that has arisen in light of the heightened fiscal desperation, as a partial (arguably inadequate) solution thereto plight. the basic principles on which the Petro is to be backed include: (1) state support through backing from reserves of natural resources like oil, gas, gold and diamonds, (2) the likelihood of international transactions, (3) registration of digital transactions through the Blockchain Observatory of Venezuela, (4) the deployment of encrypted mathematical algorithms that don't allow interception from external agents, (5) electronic transactions without intermediaries, (6) immediate transactions without commissions, and (7) instrument exchange through virtual exchange clearinghouses. The Petro is to be "controlled" or "overseen" by the Blockchain Observatory of Venezuela, attached to the Ministry of University Education, Science and Technology. An advisory role is to exist for OnixCoin, a Venezuelan

[83] IlPost (2021), "Perché l'industria dei bitcoin sta lasciando la Cina", IlPost, Internet: https://www.ilpost.it/2021/07/04/migrazione-miner-bitcoin-cina-texas/ (viewed on 20/07/21)

company that founded its own cryptocurrency. in keeping with Article 4 of Decree No. 3.196 published within the Official Gazette, a Petro is adore a "purchase-sale contract for one barrel of oil from the Venezuelan rock oil basket or any commodities decided by the state." The “underlying” backing reserves are to be the on five billion of barrels of oil from the Ayacucho I block of the Orinoco oil belt. Gold and diamonds from the Venezuelan Orinoco's mining arch also are to be certified for this purpose. Whereas the Petro represents the conceptualization of a cryptocurrency in its early stages, it does raise questions on the notions (1) government-backed cryptocurrencies, and (2) cryptocurrencies as asset-backed instruments. The cryptoanarchist philosophical roots of cryptocurrencies tend towards the disintermediation of governments from intrusion in crypto asset emission and oversight. As accountability and oversight don't seem to be primary considerations within the decentralized framework of cryptocurrencies, the thought that a government could also be the issuer of a cryptocurrency is both intriguing and concerning, since monetary authority is generally kept independent of the political architecture in many countries today, and since government-backed emission and regulation of currencies then ties the underlying value of the currency to the backing of that government. Furthermore, within the case of Petro, the currency is backed by extractive reserves, whose price fluctuates on world commodity markets. additionally, currencies require foreign legitimacy if they're to serve in international trade, and therefore the recalcitrance of external governments (e.g., US Treasury Departments) to have interaction with the cryptocurrency may hamper its effectiveness. Further still, the notion that the Petro is “monitored” and “controlled” by an “observatory” also raises questions on transparency and governance, necessitating that the Observatory and therefore the Superintendent Office maintain independence and non-partisanship[84].

However, other reasons lie behind the will to make a government-backed cryptocurrency. Even though the Venezuelan government had intentions of developing a native cryptocurrency to bypass sanctions, the U.S. still imposed sanctions on utilizing transactions with digital currencies. the foremost detrimental round of sanctions was imposed on January 2019 on PDVSA, the govt. backed oil sector of the Venezuelan economy, prohibiting engagement in transactions with the corporate (Congressional Research Service). Washington purposely imposed sanctions targeting Venezuela’s oil business to deplete Maduro from obtaining vital stream of income. Venezuela’s economic dependency on oil revenue now sanctioned by the u. s. will consequently leave a profound effect on the economy. Many fear this may worsen the devastating humanitarian crises into a catastrophe. America’s role within the global industry is sort of extensive, thus, these sanctions could prevent Venezuela from polishing off financial transactions. Maduro’s administration has developed the primary sovereign government-backed cryptocurrency to bypass sanctions, but with many challenges alongside. The administration hopes this can alleviate some epidemics the Venezuelan economy faces, especially with

[84] Chohan, U. W. (2018). Cryptocurrencies as asset-backed instruments: The Venezuelan Petro. *Available at SSRN 3119606*.

controlling pecuniary resource, and avoiding Western sanctions imposed by President Trump in 2017. President Maduro stated that his "government would issue nearly $6 billion of petros as some way to lift currency and to evade financial sanctions imposed by Washington". This development was accomplished with the help of Russia's cyber capabilities and presupposed to be a practice-run of how the CryptoRuble would operate. except for circumnavigating Western sanctions and hyperinflation, the underlying reason the Maduro administration adopted government-backed cryptocurrency is to alleviate debt. The petro is an instrument of financing for the Venezuelan government to issue debt to be traded among parties and amid the illegal promise of an oil reserve guarantee. Looking deeper into the Presidential Decrees, it absolutely was discovered the petro was an inspired tactic developed to deal with Venezuelan debt through the utilization of blockchain technology disguised as currency. These oil reserves that were allegedly presupposed to back the petro were "potential" and not yet developed. Therefore, the petro was sold at the value of Venezuelan oil basket at the time but was illegitimately backed by nothing. the most purpose of the petro was formed to relinquish the kleptocracy from exorbitant debt whereas the Sovereign Bolivar aimed to manage hyperinflation. The mismanagement in oil prices, severe hyperinflation attached to the bolivar, U.S. sanctions, intention to relinquish debt, and high amounts of corruption were catalysts for Venezuela's adoption to native government-backed cryptocurrency, the petro. Maduro's dysfunctional state behavior and desperation to bypass Western sanctions and renounce Venezuelan debt led to a failed petro. The petro is taken into account a variation of cryptocurrency; it absolutely was a promise from the Maduro regime that one petro may be traded for a physical oil barrel. The Maduro administration mislead the population to form an illusion of stability, but with the ulterior motive of addressing debt. At best, the foremost beneficial aspect of the petro is trade. as an example, the petro can commodity or services, other cryptocurrencies, or to pay the state with no rate of interest. If the state were to properly execute this, the petro could have alleviated hyperinflation and supply a stronger economic basis in Venezuela. However, given Venezuela's past of constant corruption with issuing debt and illicit drug trade, blockchain may also assist with strengthening Maduro's kleptocracy. If the distributed ledger is privatized, this can allow further corruption scandals and illicit drug trade to continue. Hence, this affirms the potential relationship between corruption and adoption of native government-backed cryptocurrencies[85].

Notwithstanding the above considerations, the petro is still failing to take off, both because of US sanctions and because of the lack of trust citizens place in the government-backed cryptocurrency itself.

[85] Mahdavieh, R. (2019). Governments' Adoption of Native Cryptocurrency: A Case Study of Iran, Russia, and Venezuela.

4.2.3 San Salvador's case

Another very recent experiment concerns San Salvador. In the Central American state since last June 2019, entrepreneur Nayib Bukele has been President. Bukele already in 2017, during his term as mayor of El Salvador, the state capital, had repeatedly expressed his interest in Bitcoin. In the same 2019, already the city of El Zonte had adopted bitcoin as its local currency, being for this reason nicknamed as "Bitcoin beach". In reality, the results related to the most famous of cryptocurrencies in El Zonte are not encouraging. Indeed, workers in the area have had numerous problems getting the application to work properly on their phones. The main problem is that El Salvador has a rather poor internet connection, which has inevitably resulted in the US dollar remaining the main and most popular method of payment. El Salvador does not have its own currency and has been using the US dollar since 2001. The date that marked the start of what was celebrated by President Bukele himself as 'historia' was 8 June 2021. About two months ago, in fact, the legislative assembly of El Salvador approved the 'bitcoin law', becoming the first state in the world to give bitcoin the status of legal tender[86].

In the 'bitcoin law' itself, there are the reasons that prompted Bukele to make bitcoin legal tender in the country: the promotion and protection of businesses, the fact that around 70% of the population does not have access to traditional financial services and, finally, that in order to promote the economic growth of the nation and increase the well-being of the majority of its inhabitants, a license is needed to make the circulation of a digital currency legal[87].

The criticism received has been manifold: firstly, the use of bitcoin is criticised given the volatility of the digital currency, secondly, according to a June 2021 survey by El Salvador's Chamber of Commerce, 92% of over 1600 respondents said they did not agree with mandating the acceptance of bitcoin, and 93.5% said they did not want to receive their salaries in bitcoin[88].

Moreover, on 7 September, the day the law came into force, numerous civilians protested in the streets of the country, expressing their opposition. However, Bukele is satisfied with the change in the country and has

[86] Nugent, C. (2021). El salvador goes bitcoin. *Time (Chicago, Ill.), 197*(23/24), 18.

[87] Diariooficial.gob.sv. (2021). Viewed on 9 September 2021, from https://www.diariooficial.gob.sv/diarios/do-2021/06-junio/09-06-2021.pdf.

[88] Hanke, S., Hanlon, N., & Chakravarthi, M. (2021). *Bukele's Bitcoin Blunder* (No. 185). The Johns Hopkins Institute for Applied Economics, Global Health, and the Study of Business Enterprise.

revealed plans to power Bitcoin mining operations in the country using geothermal energy produced by volcanoes[89].

Other concerns come from the International Monetary Fund. The UN specialised agency, which provided $389 million in emergency funding to El Salvador in April 2020, has expressed several concerns. Firstly, the IMF admitted that digital currencies have positive aspects, such as providing cheaper payments and speeding up the whole process. But implementation, says the Washington DC-based international organisation, is far from simple and requires significant investment and policy choices. Currently, the adoption of a cryptocurrency as a national currency has risks and costs that outweigh the benefits. With regard to the adoption of cryptocurrencies as legal tender, the IMF argues that the establishment of cryptocurrencies is very difficult, especially in countries with stable inflation and exchange rates, but also in less stable economies, given their high volatility and lack of connection to the real economy. Other implications would be related to monetary policy, with the central bank not being able to set interest rates on a foreign currency and with domestic prices being affected and losing stability. Finally, the IMF refers to the Financial Action Task Force (FATF), which has set a standard for regulating virtual assets and their providers in order to limit financial integrity risks[90].

A final consideration regarding the willingness to adopt bitcoin as legal tender certainly lies in El Salvador's desire to drastically reduce its dependence on the US dollar and this can be seen in relation to remittances. The adoption of bitcoin facilitates monetary transfers, given the absence of financial intermediaries and, consequently, of commissions.

In the graph below you can see that remittances have been steadily increasing over the last decade and account for more than 1/5 of the country's GDP.

[89] Odayar, T. (2021). Alternating current: El salvador to harness volcanic energy for bitcoin mining. *Power Finance & Risk.*

[90] Adrian, T., & Weeks-Brown, R. (2021). *Cryptoassets as National Currency? A Step Too Far*. IMFBlog. Retrieved 9 September 2021, from https://blogs.imf.org/2021/07/26/cryptoassets-as-national-currency-a-step-too-far/.

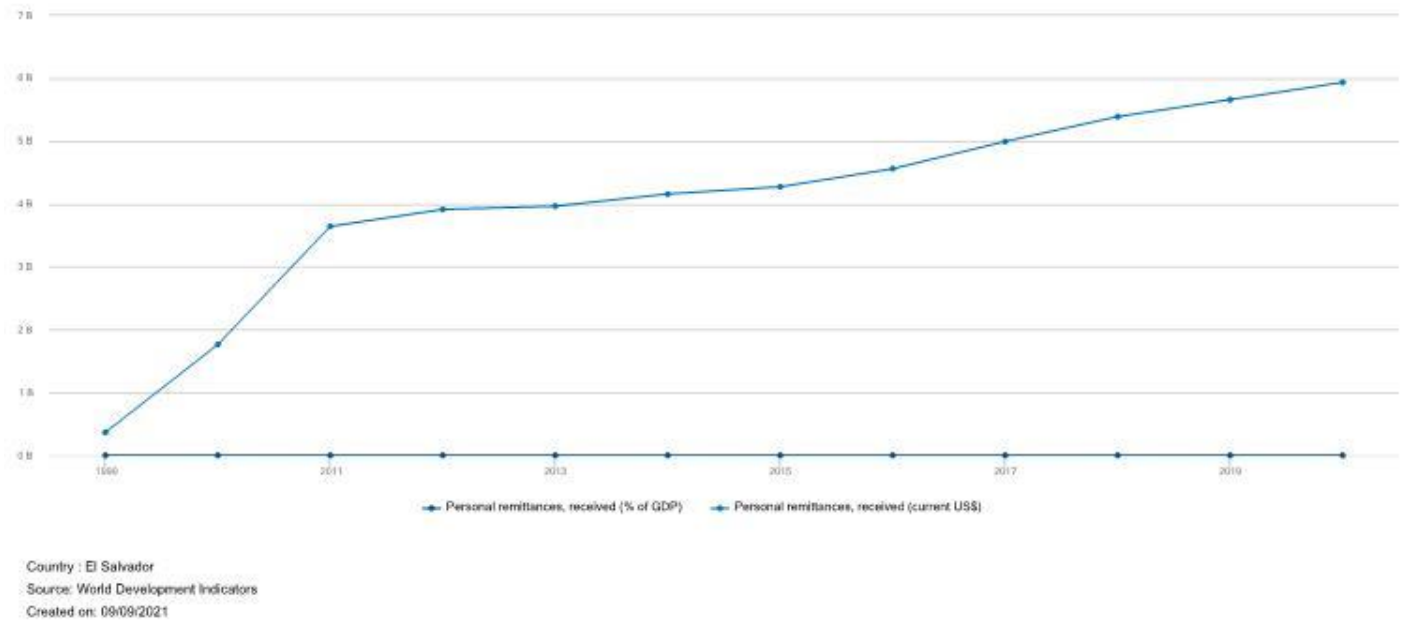


Figure 4.1 – Impact of remittances in dollars and in relation to GDP

Source: The World Bank; World Development Indicators/Data Bank; https://databank.worldbank.org/reports.aspx?source=2&country=SLV

Bitcoin has only been officially legal tender for a few days, so it is difficult to know what will happen in the short to medium term. Certainly, the beginning has been marked by numerous technical problems. The President has broad support, but there is also a section of Salvadorans who do not agree with the choice made a few months ago by Bukele and the assembly. Globally, it will be an experiment and will be observed with particular interest, especially by countries that have similar or better mining characteristics than El Salvador (natural resources, low cost of electricity, etc.). The major world financial institutions have 'warned' El Salvador and the operation has raised a number of concerns. For instance, the World Bank has already refused to help El Salvador in the rollout of cryptocurrency, as it is not considered to be something sustainable given the lack of environmental and transparency issues. Eventually, this choice will also have consequences at the political-diplomatic level, especially as regards US-El Salvador bilateral relations, already more fragile with the transition from the Trump presidency to the Biden presidency[91].

[91] Farzan, A. N. (2021,). World bank declines to help el salvador adopt bitcoin, citing environmental and transparency concerns. *The Washington Post*

4.3 Shaping the future: are cryptocurrencies the money of the future?

After analysing, in previous chapters, the history and development of cryptocurrencies, in particular the most famous of these, bitcoin, and the behaviour of some states in particular with regard to this phenomenon, it is of absolute interest and stimulus to ask a simple question: are cryptocurrencies the currency of the future? The answer, however, does not appear as simple as the question, and the aim is to provide a complete picture of both the positive and negative sides.

More in detail, the opportunities and advantages that can arise from the use of cryptocurrencies but also from one of its main features: the blockchain, will be analysed. Subsequently, what are the risks and threats related to the phenomenon and, finally, possible improvements in its use.

Certainly, this tool, which exploded during the last decade, is marking a radical change in the concept of transaction and in the use of currency, which is physically absent and intangible. However, in an age where collective consciousness and awareness has already led the majority of people to use mostly credit cards, ATMs and other digital instruments for payments of various kinds, talking about digital currencies and the physical absence of money certainly does not represent a revolution. At the same time, there are a number of factors, both economic and cultural, that by no means allow cryptocurrencies to be equated with the 'dominant' currencies today, be they physical or digital[92].

What is also true is that throughout human history people have always been attracted, intrigued and fascinated by money. Basically, the goal has always been this: the more the merrier. Just as we have seen the phenomenon of the gold rush, the way in which cryptocurrencies have become a widespread topic across the planet, and not just linked to a certain person or a certain portion of the world, leaves many experts talking about the 'cryptocurrency rush'. A race, this one, that has taken on a very different perspective and connotations, especially since, in the first years since the birth of bitcoin, the possibility of obtaining one was greater for individuals, through the infamous and already analysed mining. It is also true that nowadays, individual mining is rather difficult and above all not very profitable and, as we have already seen, it is the mining pools, the mining clouds, or at least large companies and corporations that carry out this practice. Returning to the main topic, the strong development of bitcoin, and subsequently many other cryptocurrencies, has had strong consequences in the financial world: more and more investors, industry experts, and more recently also companies, have shown a strong interest in it. This interest culminated in April 2021, when Coinbase, a platform for buying and selling cryptocurrencies, arrived on Wall Street. Between the scepticism of the large international financial institutions and central banks, which in the meantime are thinking of evolving and

[92] Árnason, S. L. (2015). *Cryptocurrency and Bitcoin. A possible foundation of future currency: why it has value, what is its history and its future outlook* (Doctoral dissertation).

creating digital currencies themselves, and the enthusiasm of the holders but also simply the admirers of the crypto project, the change is taking on new dimensions, updating itself and attempting to expand more and more[93].

4.3.1 Opportunities and advantages

The advantages and opportunities arising from cryptocurrencies are now known to most insiders and experts in the field, but also to those who want to ensure that the use of cryptocurrencies remains at its current scale and that they do not become the dominant currency.

As is well known, it was the loss of confidence in the financial sector, as a result of the 2008 crisis, that led to a growing desire for currency certainty even in the event of shocks and to ensure that the currency itself is not affected or altered by successive crises. This has led to the emergence of an alternative currency with features designed to improve the current system.

Among the qualities and advantages that are acknowledged to cryptocurrencies, there is certainly unidirectionality: within the network exchanges take place, the network itself confirms the goodness and validity of the exchange and after this, the transaction is confirmed and there is no going back. There is no need to have any documents, because, for the most part, you remain anonymous and what you need is your 'digital wallet'. Another famous feature is the absence of financial intermediaries, with all the consequences that this 'lack' brings with it: transfers are made quickly all over the planet, there are no limits on the amount, and the commissions and various related charges are low or zero. This is why cryptocurrencies are recognised as simplified transactions.

A further step forward and development that is attributed is certainly related to security: cryptocurrencies cannot, of course, be counterfeited. Furthermore, the technology used, the blockchain, complemented by the role of miners, who, as we know, recognise and validate transactions by adding 'blocks' to the blockchain, after verifying the correctness of the hash, provides the cryptocurrency instrument with a not inconsiderable security.

Blockchain technology is very secure. The crooks they will not be able to commit such a crime because several ledgers cannot be changed or validated at the same time. Among other advantages, it should be noted that the cryptocurrency algorithm is safer and better than that of credit cards. Cryptocurrencies are then operable for 24 hours 7 days a week, and this is certainly a symptom of being in step with the times, given both the evolution

[93] Burlacu, N. V. (2021). Cryptocurrencies, Money of the Future or the Future of Money. *EIRP Proceedings, 16*(1).

of the Internet of Things (IoT) and the dependence on big data. In fact, in the current state of affairs, arguing that with cryptocurrencies you "earn" two days a week to carry out all the movements is not a heresy[94].

In the graph below you can see the places of greatest interest regarding the three main cryptocurrencies in the period from 2008 to today. Although Bitcoin is the most famous and famous cryptocurrency, as also confirmed by the graph, it is interesting to note how Ethereum attracts strong interest in Rwanda, Congo-Brazzavile and Western Sahara. Ripple, for its part, attracts interests in some Commonwealth countries such as the United Kingdom, Australia and New Zealand but also in Japan and several countries of the Middle East: Afghanistan and Yemen above all.

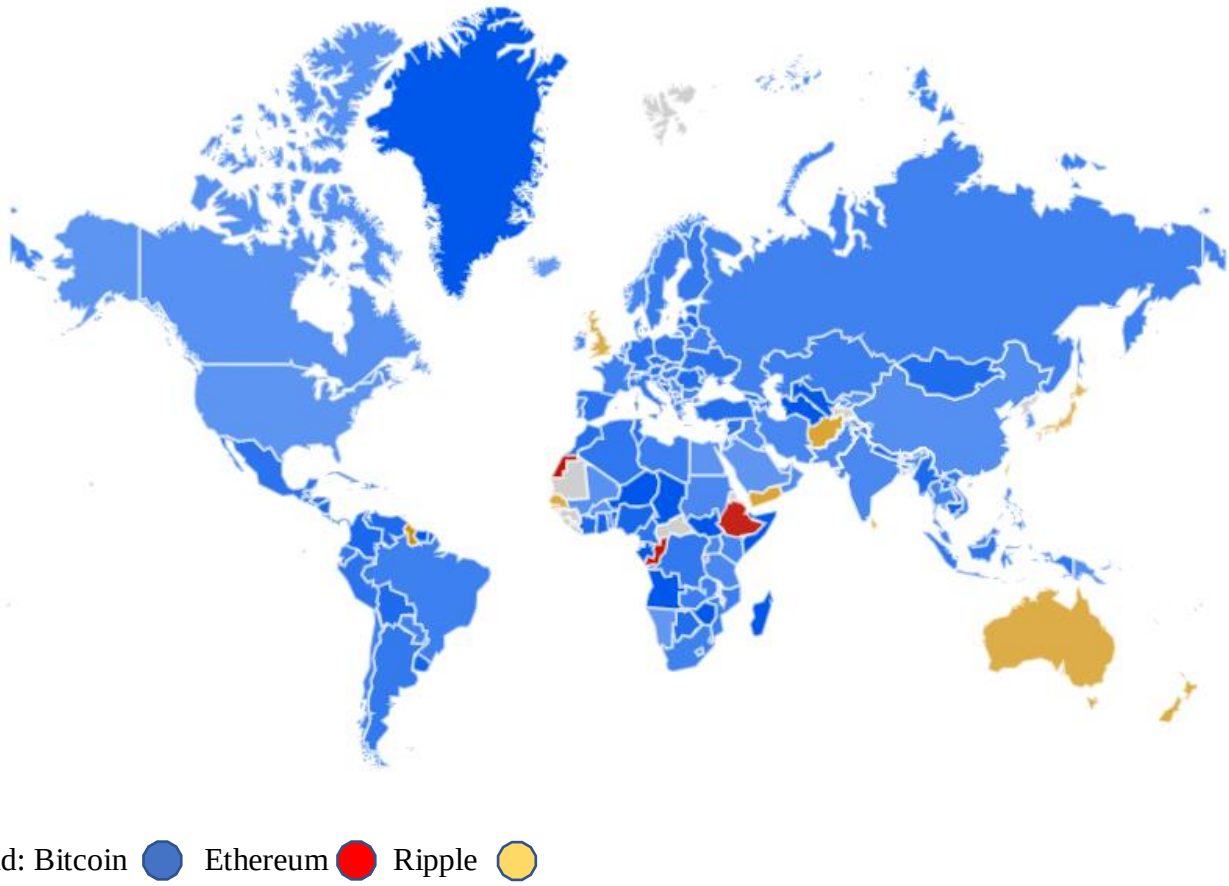


Figure 4.2 – Compared breakdown by region: interest in the three main cryptocurrencies (period 2008-present)

Source: realised with Google Trends, https://trends.google.it/trends/explore?date=all_2008&gprop=images&q=bitcoin,%2Fm%2F0108bn2x,ripple

Speaking of opportunities and advantages deriving from cryptocurrencies, it is essential to mention what is the main novelty element inherent in the phenomenon: the mechanism of the blockchain. it is possible to see that the use of the aforementioned mechanism is contributing, in many sectors, to the change of society. In the

[94] FAUZI, M. A., PAIMAN, N., & OTHMAN, Z. (2020). Bitcoin and cryptocurrency: Challenges, opportunities and future works. *The Journal of Asian Finance, Economics, and Business*, *7*(8), 695-704.

business sector in general, traditional systems are slower and more error prone, which is why intermediaries are needed. These errors are reduced in blockchain ledgers by encryption of records.

Another innovative and already in-depth element are smart contracts: These are digital with embedded if-this-then-that (IFTTT) code for self-execution. The scope is very broad, including financial premiums, insurance premiums, etc. The blockchain has its own scope of application which is also useful in health matters. Private medical records can equip themselves with this technology through encrypted archives with access available via private key for specific individuals. Additionally, the ledger can be used for drug supervision, test results, and supply management of numerous appliances and medicines. Other applications concern the financial sector and, last but not least, the government. The blockchain allows the improvement of government services and this has real consequences, such as greater transparency in the relationship between citizen and government. Even at the level of public administration and of the apparatuses that work for the greater functioning and efficiency of the State, the business processes that use the blockchain mechanism are safer and faster. The advantages also derive from a technology that brings with it a reduction in waste, an elimination of bureaucracy and the prevention of tax fraud. More generally, government proceedings are streamlined[95].

Virtually, in every area where there is an exchange, there is potential for disruption by smart contracts run on blockchain[96].

4.3.2 Risks and threats

Regarding the risks and threats associated with the use of cryptocurrencies, recent history testifies to how the phenomenon has weaknesses and aspects that probably come into play in ensuring that fiat currencies are still dominant, despite the great growth that cryptocurrencies have had over the past decade. Of course, one of the biggest risks concerns volatility: there have been numerous cases of Bitcoin and other cryptocurrencies fluctuating in relation to a simple tweet from influential people or other events that make the holding of cryptocurrencies uncertain. Critics of cryptocurrencies do not even consider it a currency due to its high volatility. Furthermore, cryptocurrencies have also suffered theft and fraud, mostly caused by faulty settings

[95] Kaur, A., Nayyar, A., & Singh, P. (2020). Blockchain: A path to the future. *Cryptocurrencies and Blockchain Technology Applications*, 25-42.

[96] Brown, G., & Whittle, R. (2020). *Algorithms, blockchain & cryptocurrency: Implications for the future of the workplace*. Emerald Group Publishing.

by exchange companies. Failure to regulate is another risk to the extent that user safety does not enjoy legislative coverage[97].

Furthermore, bitcoins and cryptocurrencies are subject to economic speculation. Some significant episodes of fluctuation related to bitcoin have led several authors to talk about the "Bitcoin bubble". Speculation is a phenomenon that is also present in the long run and, in fact, users are aware of these mechanisms, which also occur for fiat currencies, albeit to a different extent and in terms of different quantities. But what represents the greatest risk, and the greatest threat is certainly money laundering and illegal trafficking. More generally, we are talking about the illicit use of cryptocurrencies. We will have the opportunity to explore this topic in the next chapter, however, this problem did not arise with cryptocurrencies, there have been online platforms for some time that simulate an internal monetary system in order to cover up illegal criminal acts. However, the quasi-anonymity feature of cryptocurrencies has certainly made a dent in the possibility of criminal use to facilitate illicit behaviour. Moreover, as is well known, cryptocurrencies are not all the same, and in some, traceability is even more complicated than it normally is. All this, of course, originates as an aspect of guarantee and security of the clients, but has negative consequences if the analysis is aimed at studying the so-called 'dark sides' in the use[98].

Despite the divisions, between those who consider cryptocurrencies unsuitable for this use, because malicious actors would need strong, non-volatile currencies and because transactions are publicly recorded in the ledger, and those who consider this type of currency perfect for dirty money transfer operations, the threat and risk exists. The existence of these risks and threats becomes 'real' when a tool like cryptocurrencies, which makes quasi-anonymity a peculiarity, mixes with the deep web. The deep web, which according to some experts represents about 99% of the total web, is composed of a conspicuous set of sites, and access to it does not take place in the conventional way. Either specialised software (used anonymously) is required for access, or networks that mask identity, or Internet Protocol (IP) addresses. It is in the dark web, considered as a part of the deep web where access is closed and exclusive, that the dark side of globalisation and the revolution that came with the advent of the internet exists. In a large part of the markets where illicit exchanges take place, only bitcoins or other cryptocurrencies are accepted by sellers, in order to ensure a more solid anonymity and to evade or complicate investigation processes. In this respect, the table below on five deep web marketplaces

[97] DeVries, P. D. (2016). An analysis of cryptocurrency, bitcoin, and the future. *International Journal of Business Management and Commerce*, *1*(2), 1-9.

[98] Brezo, F., & Bringas, P. G. (2012). Issues and risks associated with cryptocurrencies such as Bitcoin.

is of particular interest. What immediately catches the eye is certainly the fact that all marketplaces considered accept bitcoin, with one of them probably also accepting other cryptocurrencies[99].

Table 4.2 – A Summary of five Deep Web Marketplaces

	BlackBank	Hydra	Black Market	Outlaw Market	Silk Road 2.0
Typology of Available Products	Alcohol, Counterfeits, Drugs, Fraud guides and tutorials, Tobacco	Apparel, Digital goods, Drugs, Services, Tobacco, Weapons, Custom Orders	Drugs, Fraudulent Documents, Weapons	Digital Goods, Drugs, Electronics, Services	Alcohol, Drugs, Drug paraphernalia, Erotica, Lotteries, Money, Services
Number of Drug Listings	268 (drugs)	1,725 (drugs/tobacco)	3 (drugs)	140 (drugs/tobacco)	13,383 (drugs)
Bitcoin Accepted?	✓	✓	✓	✓	✓
Other Cryptocurrency Accepted?	✗	✗	✗	✗	?
User Discussion Forum?	✓	✗	✗	✓	✓

Source: anser.org. 2014. *Risks and Threats of Cryptocurrencies*. [online] Available at: <https://www.anser.org/docs/reports/RP14-01.03.03-02_Cryptocurrencies%20508_31Dec2014.pdf> [Accessed 11 September 2021].

Other risks and threats related to cryptocurrencies, such as money laundering, fraud and, above all, evasion of sanctions, will be discussed in more detail in the next chapter.

4.3.3 Possible improvements

With regard to possible improvements in cryptocurrencies, it is clear that these are related to the risks and threats analysed in the previous section. Reduction is the key element and would already represent a significant improvement. Equally clear is the difficulty of this improvement, especially since illicit use occurs through and because of the unique and peculiar characteristics that cryptocurrencies have. The challenges are numerous, and can be grouped into five categories: security threat; danger of virtual money system collapse; impacts of real-world monetary systems; money laundering, tax evasion and online criminal; value fluctuation of virtual money. As far as the phenomenon of tax evasion is concerned, this occurs mainly because of a lack of regulation, laws and control systems. Clearly, the absence of a central entity, another key feature of

[99] anser.org. 2014. *Risks and Threats of Cryptocurrencies*. [online] Available at: <https://www.anser.org/docs/reports/RP14-01.03.03-02_Cryptocurrencies%20508_31Dec2014.pdf> [Accessed 11 September 2021].

cryptocurrencies, means that it is governments and international organisations that are responsible for legislating in this regard[100].

Another challenge, perhaps the most important, is acceptance by the general public. Any massive acceptance would, firstly, constitute further growth for the entire sector and, secondly, would put more pressure on banks and central governments to implement measures, although many governments and banks, as we have already seen, have already moved or expressed their views. Certainly, the fear of the latter lies in the loss of control. While supporters of the distributed cryptocurrency system have full confidence in the currency, the lack of a central authority is an uncertainty for many others. Not knowing who is behind it, or at any rate knowing that it is users as they might be, and not people within a developed and politically and institutionally trusted entity, does not make for trust. This is the step that cryptocurrencies failed to take in the last century during their evolution. In this sense, it is interesting to note that, at present, the willingness to use a cryptocurrency as an actual currency, especially if managed by a private company, remains very low. As you can see from the chart below, there are several reasons for this: except in the United States and the United Kingdom, lack of trust is the most important reason. Moreover, except in Germany and Spain, in all other countries included in the survey more than 30% of people prefer the central bank to control and manage the money flow[101].

Figure 4.3 – Reasons for not supporting a new cryptocurrency

Source: CGC, Cryptocurrencies and The Future of Money: International Survey.

[100] Richter, C., Kraus, S., & Bouncken, R. B. (2015). Virtual currencies like Bitcoin as a paradigm shift in the field of transactions. *International Business & Economics Research Journal (IBER)*, *14*(4), 575-586.

[101] CGC (2019), "Cryptocurrencies and the Future of Money", *Center for the Governance of Change*, Madrid: IE University.

Another challenge concerns what the greatest innovation is perhaps inherent in cryptocurrencies: the blockchain. As already explained, numerous fields of application have already integrated this mechanism, and now the challenges of the future essentially boil down to the following two: to implement this use even more in fields where it is not yet present, and, at the same time, to improve and make users more ready and able to use blockchain technologies. Another direction would be to implement the fields of application, exploiting the value to facilitate procedures, but with individuals retaining control of the data and deciding for themselves how and when to make them available to third parties[102].

It follows from the brief analysis that challenges will be numerous in the near future, many of them difficult to overcome as they impact and make use of the main features of cryptocurrencies. Certainly, for there to be tangible improvements, the involvement of institutions at both national and international level will be necessary.

[102] Makridakis, S., & Christodoulou, K. (2019). Blockchain: Current challenges and future prospects/applications. *Future Internet*, *11*(12), 258.

Chapter 5

How cryptocurrencies are used to escape from sanctions

5.1 The phenomenon of sanctions evasion

As already mentioned, cryptocurrencies, like all innovations in history, bring with them positive sides but also shadows and negative consequences, especially if they are used by terrorist and/or criminal organisations. Money laundering, the use of the instrument to finance terrorist organisations, the use of the dark web to buy drugs, weapons and other illicit material, and tax evasion are all criminal activities that involve the use of cryptocurrency, exploiting its quasi-anonymity and decentralisation.

However, this chapter will focus on one specific topic: sanctions evasion through cryptocurrencies. Obviously, in order to analyse the latter in its entirety and complexity, it is necessary to start by studying the evasion of sanctions, and then implement the analysis by adding the relatively new phenomenon of evasion through cryptocurrencies.

There have been cases in the past where individuals or more complex entities tried to help a foreign government by disguising transactions in order to evade sanctions imposed on one state by another or by an international organisation. What is essential to know is the close relationship between sanctions and the international payment system. Through the latter, sanctions are implemented simply, directly and effectively. Disconnecting a country from the international payments system is one of the most powerful economic weapons. Today, SWIFT (Society for Worldwide Interbank Financial Telecommunication) plays a major role in this respect. Established in the late 1970s, SWIFT makes it possible to send and receive payments in a standardised form. The group of banks operating SWIFT is mostly from Europe and North America. Especially with regard to the United States, SWIFT has assumed an increasingly important role since 2001, when it was used to trace the financing network of Islamic fundamentalists after the attack on the Twin Towers. In 2012, again under American pressure, SWIFT disconnected the Iranian banking system from the payment network. The action was part of the sanctions package aimed at stopping Iran's nuclear programme. When, as we have already seen, under President Trump the US withdrew from the JCPOA, reactivating sanctions against Iran, the European Union decided to set up INSTEX (Instrument in Support of Trade Exchanges) precisely to encourage trade with Iran, since Iran had again been cut off from SWIFT. The United Nations, in 2017, also ousted three North Korean banks from SWIFT, pursuant to Resolution 2371/2017. More generally, what can

be argued with certainty is that SWIFT is the most powerful weapon in the field of sanctions, and there are numerous emblematic cases in this respect[103].

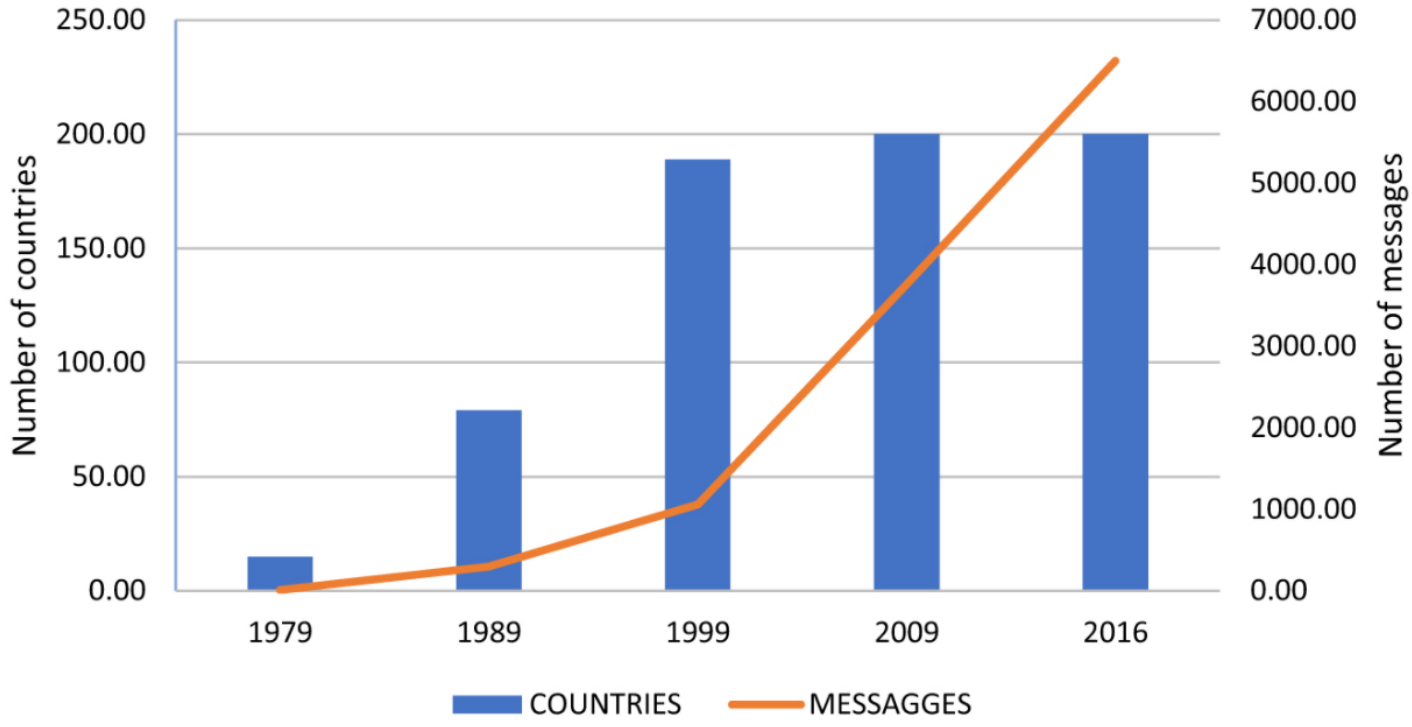


Figure 5.1 – SWIFT evolution over time

Source: Fantacci, L., & Gobbi, L. (2021). Stablecoins, Central Bank Digital Currencies and US Dollar Hegemony. *Accounting, Economics, and Law: A Convivium*.

The idea of using sanctions as an instrument of 'covert warfare' is by no means new. The history of international organisations teaches us this. Sanctions were already being used by the League of Nations, although their effectiveness was weak or non-existent. What, in the recent past, has changed and is changing, is the attempt to circumvent sanctions through the use of the new instrument of cryptocurrencies, which has seen its growth also in capacities connected to their use and, among these, some States have learnt also that relative to the circumvention of sanctions[104]. In order to provide a broad and accurate picture of the phenomenon, the question to start with is: where were sanctions have been evaded and how? In fact, despite being rather recent, sanctions evasion through the use of cryptocurrencies has several well-documented cases and the literature is quite dense. Rogue regimes and revisionist powers have sought and still use digital currencies with the aim of weakening and circumventing the power of US sanctions. Russia, Venezuela, China, Iran and North Korea are at the forefront of attempts to implement national cryptocurrencies. This evasive manoeuvre allows them to

[103] Fantacci, L., & Gobbi, L. (2021). Stablecoins, Central Bank Digital Currencies and US Dollar Hegemony. *Accounting, Economics, and Law: A Convivium*.

[104] Verdier, P. H. "A Hidden War": Sanctions Evasion. In *Global Banks on Trial* (pp. 109-146). Oxford University Press.

circumvent global supervision of financial transactions and weaken the US dollar. The common theory is that through the quasi-anonymity of cryptocurrencies (which then varies depending on the digital currency in question), US hegemony will no longer be so because the ability to control the flow of financial movements both inside and outside the sanctioned countries will be much less. Cryptocurrency payments make it possible to bypass the financial controls established as part of sanctions enforcement[105]. Russia, Iran, Sudan, North Korea and Venezuela are countries on which the US has imposed economic sanctions, obviously for different reasons. In these countries, the use of digital currency as a tool to circumvent sanctions has increased, and different strategies and methods are being used. We will have the opportunity to analyze the methods and strategies later. What interests us in this brief overview revolves around the observation that various states circumvent economic sanctions through this instrument, which made it necessary to have "crypto-sanctions" and measures taken by the affected states. These measures are, precisely, crypto-regimes, which try to respond and regulate events and try to prevent even what could happen in the future.

5.2 European Union and United States crypto-regime

Such strong and rapid growth and evolution, as experienced by cryptocurrencies, naturally brings with it various questions about risks and benefits, as we have already analysed. What is of interest in this section is to focus on the crypto regime in the United States and the European Union. In order to understand the regulatory side of the cryptocurrency market, it is essential to first define cryptoassets and how they interact with the financial market. Cryptoassets are nothing more than a different form of fintech innovation that inevitably has an impact on the financial sector. Given the exponential growth that cryptocurrencies have had over the past decade, it is increasingly inevitable to talk about regulation, not least to ensure a range of market protections. It is interesting to study the different regulatory approaches that can be applied, as well as possible regulation at a global level. The question is: how can financial innovation be improved and promoted without undermining stability and, at the same time, protecting investors? What can immediately be concluded to be a paradox is the following: the international financial market has a global reach, while national and regional initiatives have limited power to manoeuvre. As we will elaborate later, an example of transnational initiatives concerns the recommendations made by the Financial Action Task Force (FATF) on virtual currencies[106].

[105] Dudley, S., Pond, T., Roseberry, R., & Carden, S. (2019). Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency. *Joint Forces Quarterly*, *92*(1), 60.

[106] Jovanić, T. (2020). An Overview of Regulatory Strategies on Crypto-Asset Regulation-Challenges for Financial Regulators in the Western Balkans. In *Tatjana Jovanić, An Overview of Regulatory Strategies on*

As far as the European Union is concerned, the picture is rather complex. In fact, several paths have been taken, especially by the European Commission and the Central Bank, in response to numerous events and 'criminal' uses of cryptocurrencies. First of all, a joint declaration of the two bodies has established how they are continuing their efforts to ensure a European digital financial sector in order to respond to the new needs of consumers. The ECB is considering issuing a digital euro. The consultation took place on 12 January 2021, and, after a period of preparatory work, the ECB will assess whether the project can be launched. What needs to be emphasised is that crypto-assets have already been subject to EU legislation on securities markets. However, the emergence of digital ledger technology (DLT) and crypto-assets themselves (which do not qualify as 'financial instruments', such as utility tokens or payment tokens) came later. The Commission has therefore proposed a pilot regime for market infrastructures willing to trade and settle transactions in financial instruments in the form of crypto-assets. The proposal, which dates back to September 2020, aims to provide legal certainty and flexibility to market participants wishing to operate a DLT market infrastructure by establishing uniform requirements for the operation of such infrastructures. The subject and scope, terms, definitions are defined. It also sets out the requirements for a DLT MTF and ensures consistency with existing policy provisions in this area and other Union policies. Finally, the supervision and cooperation of competent authorities and ESMA. ESMA will, at the latest after a period of five years, report to the Commission on the pilot scheme and, on the basis of ESMA's assessment, the Commission will prepare a report including a cost-benefit analysis in order to determine whether this scheme can be maintained or will need to be modified[107].

With regard to the aforementioned crypto-assets that are not classified as 'financial instruments', the Commission has proposed a new specific framework. This would replace all other EU and national rules currently governing the storage, trading and issuance of crypto-assets. The framework is Markets in Crypto-Assets Regulation (MiCA). The proposal would amend EU Directive 2019/1937 and is part of the Digital Finance package, where the just mentioned pilot regime on distributed ledger technology (DLT) market infrastructures is also included. The proposal aims to provide first and foremost legal certainty regarding cryptocurrencies not covered by existing EU financial services legislation, as well as to establish uniform rules for cryptocurrency service providers and issuers in the EU. The proposed regulation is divided into nine titles. The subject matter, scope and definitions are defined. It also regulates the offering and marketing

Crypto-Asset Regulation-Challenges for Financial Regulators in the Western Balkans, in: EU Financial Regulation and Markets-Beyond Fragmentation and Differentiation (Eds. I. Bajakić, M. Božina Beroš), Conference Proceedings, Zagreb.

[107] European Commission. (2020). *Proposal for a Regulation of the European Parliament and of the Council: On a pilot regime for market infrastructures based on distributed ledger technology*, COM/2020/594 final, 24.9.2020, Brussels

to the public of crypto assets other than asset-referenced tokens and e-money tokens. More generally, the framework is certainly updated, making it more up-to-date. Details are also provided on the powers of the competent national authorities. An obligation is imposed on Member States to designate one or more competent authorities for the purposes of the Regulation, including a competent authority designated as a single point of contact. What is of most interest for the purposes of this analysis is Chapter 2 and, in particular, a number of articles imposing obligations to act honestly, fairly and professionally, organisational requirements, prudential safeguards and rules on the safekeeping of cryptocurrencies and client funds[108].

In the European context, the work carried out by various bodies should be emphasised, especially with regard to the use of crypto-assets for money laundering. The fifth directive is already in place, which shows how the EU is trying to keep up with a rapidly evolving sector. What can be sustained, however, is the lack of close and strong cooperation between the FATF (Financial Action Task Force) and the EU itself regarding even shared definitions for money laundering and, subsequently, attempt to implement common actions. The AMLD5 (Anti-Money Laundering Directive) came into force last January 2020, however, it needs some adjustments and updates also in relation to the evolution of the whole sector. In the wake of the FATF, the definition of virtual currencies needs to be broadened to include tokens. In addition, the inclusion of 'state currencies' and 'in-game currencies' would also be necessary, as well as the exchange from crypto to crypto, the inclusion of trading platforms and the provision of financial services[109]. Just six months after AMLD5, the European Union published its sixth directive on the subject. The main objectives are to achieve greater clarity and harmonisation between the EU Member States. In addition, as money laundering is still not widely reported, the directive will also increase the reporting obligations of Member States[110]. More recently, about a couple of months ago, the European Commission decided to tighten the rules on cryptocurrency transfers. Companies transferring bitcoin or other cryptoassets will have to collect details of senders and recipients in order to help the relevant authorities crack down on dirty money. This is a further regulation of the sector after AMLD6 and implements a recommendation from the FATF[111].

In conclusion, what can be argued is that the European Union is progressively making more and more efforts to regulate such a large, complex and constantly evolving sector. The anti-money laundering directives are

---

[108] European Commission (2020). *Proposal for a Regulation of the European Parliament and of the Council: On a Markets in Crypto-assets, and amending Directive (EU) 2019/1937,* COM/2020/593 final, 24.9.2020, Brussels

[109] Houben, R., & Snyers, A. (2020). *Crypto-assets: Key developments, regulatory concerns and responses*.

[110] Hagen, J. (2021). *6AMLD the Five Key Changes*. Skillcast.com. Retrieved 16 September 2021, from https://www.skillcast.com/blog/6amld-key-changes.

[111] Jones, H. (2021). *EU to tighten rules on cryptoasset transfers*. Reuters. Retrieved 16 September 2021, from https://www.reuters.com/technology/eu-tighten-rules-cryptoasset-transfers-2021-07-20/.

constantly being updated, as is the idea of making numerous changes using blockchain technology. The European Union has created the European Blockchain Partnership to build the European Blockchain Services Infrastructure (EBSI), with the aim of improving cooperation between member states and providing citizens with more efficient services using blockchain technology.

In the United States of America, the Office of Foreign Assets Control (OFAC) of the Treasury Department administers and enforces economic sanctions under US law. Sanctions must be complied with by all US persons, both US citizens and permanent resident aliens. OFAC itself has, since 2018, initiated measures to counter this phenomenon. There are, in addition to OFAC, other regulators in the United States, such as the Financial Crimes Enforcement Network (FinCEN), which is also part of the Treasury Department. FinCEN already clarified in 2013 that administrators and those who trade in virtual currency are equated with money transmitters for money services activities and therefore have an obligation to implement AML record keeping, reporting and compliance measures. FinCEN itself issued a warning in 2018 related to Iran's attempts to exploit the international financial system, with the intention of alerting US financial institutions to better detect potentially illicit transactions involving the Middle Eastern state. Although cryptocurrency use at the time was relative in Iran, the action was intended to alert the emerging use that could provide avenues to evade sanctions. In general, the US government is particularly concerned that sanctioned countries or parties have been using cryptocurrency to circumvent sanctions and subsequently facilitating illicit activities such as money laundering and ransomware attacks. OFAC has significantly increased its presence in the sector in order to regulate it by emphasising compliance obligations; these remain the same whether transactions are denominated in virtual or fiat currency, and has begun to include in its list of Specially Designated Nationals and Blocked Persons (SDNs) virtual currency addresses linked to sanctioned persons. These are enforced with the help of banks and companies that have implemented systems and controls internally to detect and block these illicit activities. Regarding recent events, last March 2020, the US Department of Justice indicted Chinese nationals Jiandong Li and Yinyin Tian for laundering cryptocurrencies worth more than $100 million by hacking a cryptocurrency exchange. In a coordinated action, OFAC designated Li and Tian as SDNs and added 20 new bitcoin addresses associated with these two individuals to the SDN list. The civil forfeiture complaint specifically names 113 virtual currency accounts and addresses that were used by the defendants and anonymous conspirators to launder funds. Li and Tian stole $250 million in cryptocurrency by hacking a virtual currency exchange. To then launder funds, Li and Tian circumvented compliance checks at various virtual currency exchanges by submitting falsified "know your customer" information and used "peel chains" to launder the stolen cryptocurrency and obscure the source of the funds. In a peel chain, criminals "peel" off a small amount of cryptocurrency from a larger amount during a transaction. The process is repeated until all of the cryptocurrency has been sent to new addresses and it is often deposited into various virtual currency exchanges. Li and Tian spent several

months using peel chains to transfer and convert much of the stolen cryptocurrency into regular currency at Chinese banks. The pleadings also indicate that Li and Tian sold some of the stolen cryptocurrency to U.S. customers and routed some of the funds through a U.S.-based cryptocurrency exchange[112].

The emerging and evolving regulatory framework makes most virtual currencies and many cryptocurrency issuers subject to anti-money laundering regulations, as well as wallet providers. States may also apply licensing and regulatory requirements, as, for example, New York State has done with the Department of Financial Services' "Bitlicense" regulation. As regards the structure of anti-money laundering regulation of cryptocurrencies, this is more developed for centralised virtual currencies. As argued above, uniform rules for the adoption of global anti-money laundering standards for cryptocurrency trading have not yet been achieved. However, there is agreement and convergence on the FATF's position: cryptocurrency payment service providers should be subject to the same obligations as fiat currency payment service providers. However, there are a number of differences in national approaches to the problem and they revolve around: the existence of special licensing requirements for virtual currencies; the extent to which crypto-to-crypto exchange is regulated differently from crypto-fiat exchange. Instead, most jurisdictions have issued regulations or guidelines with the aim of ensuring that commercial exchange of cryptocurrencies for fiat currency (including through virtual currencies) is subject to anti-money laundering requirements or, as in China, even prohibited[113].

OFAC publishes a list of individuals or entities that have violated or attempted to violate, or conspired to violate, or caused a violation of US sanctions. These individuals or entities are listed on the Foreign Sanctions Evaders (FSEs)[114]. Transactions by US persons or within the US involving members of FSEs are prohibited. OFAC (Office of Foreign Assets Control) began implementing its work in the cryptocurrency sector from November 2018, when digital currency addresses linked to the Specially Designated Nationals and Blocked Persons List were listed. it was, this, the first time in which cyber-related sanctioning authorities were used. OFAC has also published best-practices to follow regarding cryptocurrency compliance, with all aspects to be considered by each department. OFAC is therefore pushing for the

---

[112] Group, G. (2021). *Sanctions 2021 | Rising Risk: Recent Developments in Cryptocurrency Sanctions and Enforcement | ICLG*. International Comparative Legal Guides International Business Reports. Retrieved 16 September 2021, from https://iclg.com/practice-areas/sanctions/3-rising-risk-recent-developments-in-cryptocurrency-sanctions-and-enforcement.

[113] Holman, D., & Stettner, B. (2018). Anti-Money Laundering Regulation of Cryptocurrency: US and Global Approaches. *Електронний ресурс]/D. Holman, S. Barbara//Allen & Overy LLP.–2018.–Режим доступу до ресурсу: http://www. allenovery. com/publications/engb/Documents/AML18_AllenOvery. pdf*.

[114] *Office of Foreign Assets Control - Sanctions Programs and Information*. U.S. Department of the Treasury. (2021). Viewed on 18 September 2021, from https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information .

cryptocurrency space to be prepared to enforce the sanctions regime in place in other industries. Furthermore, the prosecution of states such as Iran or other 'rogue regimes' that evade sanctions through cryptocurrencies will be widespread. This will of course also be done against companies that lend themselves to this dishonest and criminal practice. As an example, last February, BitPay Inc, a payment processing company that accepted cryptocurrencies entered into a settlement of about half a billion dollars with OFAC for more than 2 thousand violations of multiple sanctions programs. The company had allowed transactions with U.S. merchants and others in North Korea, Iran, Syria and other areas subject to U.S. sanctions. In the United States, the Office of Comptroller of the Currency confirmed in an interpretative letter last January that banks may use stable coins in conducting payment transactions for customers[115]. This is part of a perspective in which the Office of Comptroller of the Currency wants to try to take advantage of new technologies emerging from cryptocurrencies. The response from the industry has been convincing and financial institutions need to ensure that, despite the incorporation of this technology, it should not be used in disregard of AML/CFT compliance obligations[116].

5.3 Actors: who escapes, how and why? A geopolitical bond

By studying the actors involved in the evasion of sanctions through cryptocurrencies, it is possible to understand how the phenomenon is inevitably linked to geopolitical factors. it is necessary to underline how the actors can be: States, and we will have the opportunity to deepen in the course of the chapter which States in particular, but also commercial businesses and individuals. The cases referred to, where there is currently more documentation and, consequently, more truthfulness, refer to cases of evasion committed by the United Nations or the United States of America.

The flourishing of this practice, as mentioned many times before, is due to particular characteristics that cryptocurrencies possess, more specifically: pseudo-anonymity and the limited presence of third-party intermediaries. As regards pseudo-anonymity, this has already been discussed above. Bitcoin, like many other cryptocurrencies, possesses a significant degree of inherent anonymity. The public key of each Bitcoin user is encrypted in order to produce a public address. The public is therefore able to see who is sending and receiving

[115] *Current Trends and Ofac's Best Practices for Compliance - Association of Certified Sanctions Specialists*. Association of Certified Sanctions Specialists. (2021). Retrieved 19 September 2021, from https://sanctionsassociation.org/sanctions-in-the-cryptocurrency-space-current-trends-and-ofacs-best-practices-for-compliance/.

[116] ComplyAdvantage. (2021). *A New Sanctions Regime and a Spotlight on Crypto*. Retrieved 18 September 2021, from https://complyadvantage.com/blog/a-new-sanctions-regime-and-a-spotlight-on-crypto/ .

transactions, as well as the amount of cryptocurrency transferred. However, no personally identifiable information about the actors involved in the transactions is included. This internal mechanism has allowed companies in sanctioned countries to exploit cryptocurrencies - in most cases Bitcoin - in order to evade financial sanctions. As regards the limited presence of third-party intermediaries, there are several considerations in this regard. First, few of these third-party authorities have any real ability to cancel or freeze digital currency payments. Moreover, the likelihood that they will exercise their powers to monitor such exchanges is very low. There is another key consideration: intermediaries' profit from their users' cryptocurrency transactions. Blocking an exchange would therefore disrupt the income stream of intermediaries. Here the mechanism merges with the problem of sanctions evasion: even assuming that the intermediary is aware of the illicit nature of the digital currency exchange, the incentives to stop it are minimal. What happens, more likely, is the exact opposite: financial intermediaries may have an incentive to make sure that users located in sanctioned countries are satisfied. Amongst others, this is the case of Iran, which we will analyse shortly, where Bitcoin has become a way to circumvent US sanctions and intermediaries have used the opportunity to match buyers in Iran with sellers in countries all over the globe. Despite the difficulty of restricting the practice, what should be in place is an obligation on the part of states to stop trading with bad actors within the international sphere. This is because the aim of sanctions at the economic level is not solely to punish the state for the transgressions committed, but to ensure that a change in the behaviour itself can be promoted, after becoming aware of the impropriety at the ethical-legal level. It is the international community that, therefore, must assume the obligation to repress unhealthy and illegal behaviour, not least so as not to risk being an accomplice to it. In continuing the link with customary international law, it is essential to mention the principle of "nullus commodum capere de sua injura propria" (you cannot take advantage of your own wrong). What is identified here as a wrong is the absence of regulation of cryptocurrencies or regulation that is inadequate and out of step with the phenomenon, which is constantly evolving and liable to change. Clearly, where there is no regulation, evasion and malfeasance thrive, and all states that fail to combat evasion of sanctions, despite being in a position and willing to do so, profit from it. The profit comes from the advantage of freeing up compulsory state resources, the wrong is, as just explained, the refusal to regulate cryptocurrencies effectively and virtuously, in order to reduce sanctions evasion. Clearly, detractors of the legal doctrine and customary international law argue that if economic sanctions are not themselves legal and justified, then the principle falls apart and we are moving in the direction of a 'just war'. Beyond the legal issues, what is of interest is the limitation of financial sanctions evasion through cryptocurrencies. In this sense, the main actors are the states. North Korea is currently using cryptocurrency revenues to support its nuclear weapons programme. International organisations such as the European Union and the United Nations have imposed bans on transactions with companies and individuals. The imposition of sanctions is symptomatic of the seriousness and concern of the situation. Allowing cryptocurrencies to be used in an uncontrolled manner undermines the effectiveness of financial sanctions. All this is facilitated by an exquisitely geographical aspect:

the place where all this is happening. Digital is an aspect of the problem insofar as the public is often blind to the number of countries sanctioned, the individuals, companies and corporations involved and who repeatedly implement this practice. On the other hand, if it is true that transactions are public, going to identify transactions within the blockchain is a very complicated process and certainly not done by simple users of the network. Another problem stems from the use of cryptocurrency in the world, as the more accessible cryptocurrency is, the more access those who avoid sanctions have in global financial markets[117].

Regarding North Korea, there is a long history linking the country with both the United Nations and the United States and US sanctions. Since 1953, there have been numerous episodes of escalation and tensions in the bilateral relationship between the two states. For its part, the UN first imposed sanctions on North Korea in 2006, while the US had been having conversations and meetings about denuclearisation since the 1990s. What has actually happened is that the sanctions imposed by the US on North Korea in recent years, such as the possibility of sanctioning individuals and entities involved in the trade of minerals or metals or even sanctioning people who provide support to UN-sanctioned persons, have led to enormous financial difficulties for the Asian state. What followed, given that the currency of trade around the world has traditionally been the US dollar, was a strong involvement in state-sponsored cybercrime. In addition, the country also started practising cryptocurrency theft. The field of cybercrime has been practised by North Korea for several years, but the one implemented with the involvement of cryptocurrencies is quite new. DPRK has been involved in cybercrime for many years, but their hacking of cryptocurrency exchanges is fairly new. The first reported hack of a crypto by DPRK was reported in February 2017. An exchange called Bithumb was hacked for around $7million worth of cryptocurrency. Later in the year, North Korea was blamed for hacking of the exchange YouBit, which later went bankrupt from losing 17% of its assets. In May 2017, North Korea conducted the WannaCry Bitcoin ransomware attack, earning at least $120,000 USD worth of Bitcoin in exchange for unlocking victims' systems. The figure below shows the process carried out in the WannaCry attack and how Bitcoin is involved.

[117] Macfarlane, E. K. (2021). strengthening sanctions: Solutions to curtail the evasion of international economic sanctions through the use of cryptocurrency. *Michigan Journal of International Law, 42*(1), 199-229.

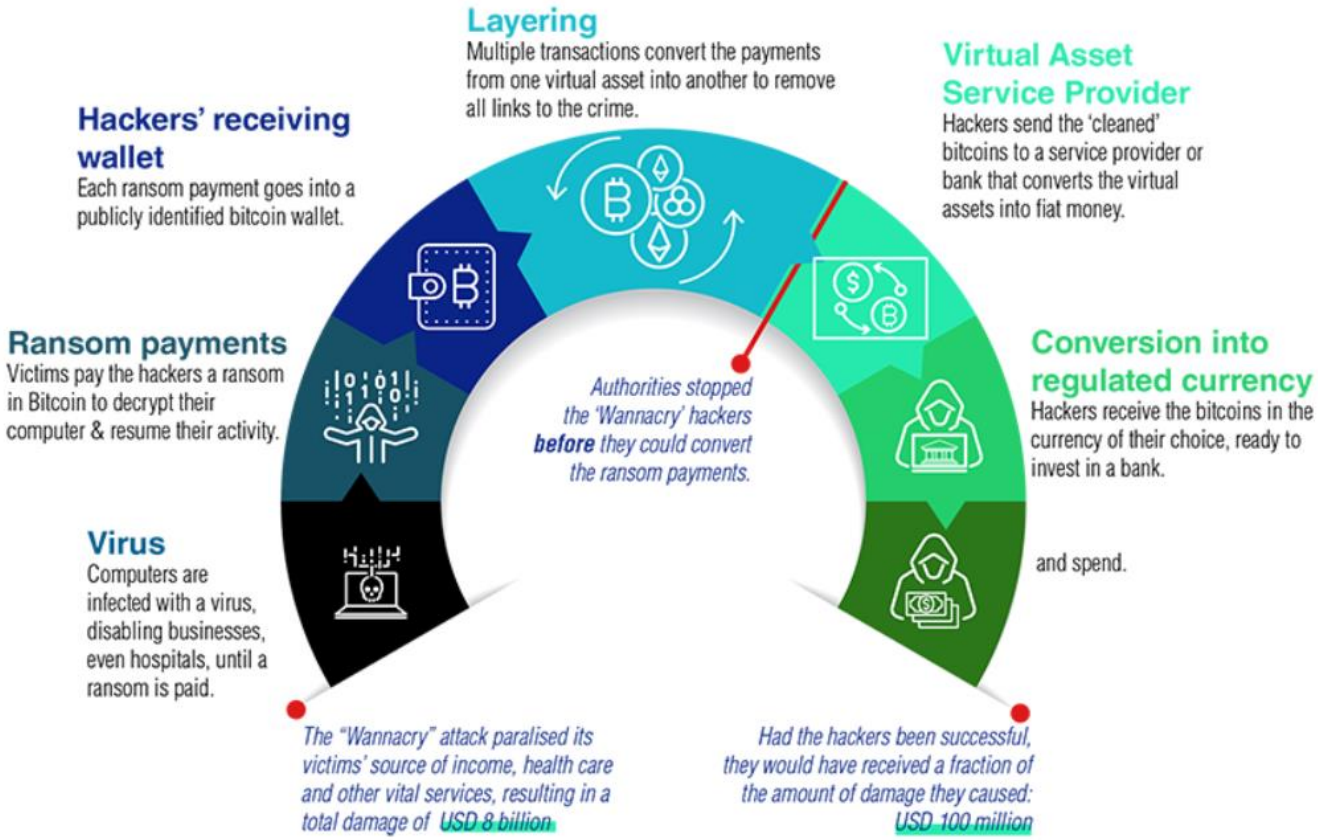


Figure 5.2 – WannaCry attack process

Source: *Documents - Financial Action Task Force (FATF)*. Fatf-gafi.org. (2021). Retrieved 20 September 2021, from https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate).

Other sources cite that DPRK obtained 11,000 Bitcoins in 2017; because of the volatile nature of Bitcoin this has been worth anywhere from $39.9 million to $210 million. More recently, North Korea is a primary suspect in the heist of a coin called NEM from the crypto exchange Coincheck located in Japan. On January 26th, 2018, hackers stole $526 million worth of NEM which has since been traced back to North Korea. On that day, NEM was worth about 83 cents each and on March 7th, 2018, one NEM coin was worth about 34 cents each; up to April 2019, the price has not recovered to the pre-hack price. One international cyber security company, Group-IB, published that five cryptocurrency exchange attacks are linked to Lazarus, a North Korean state sponsored hacking group. (Group-IB, 2018). These cyber-attacks tied back to North Korea are not the only thing showing the country has a growing interest in the field. A panel of experts to the UN Security Council in March 2019 reported that North Korea cyber-attacks and thefts have resulted in the country amassing approximately $670 million in foreign and virtual currency. Democratic People's Republic of Korea cyber actors steal cryptocurrency, use it to launder proceeds in evasion of financial sanctions and mine it through cryptojacking attacks for the purposes of revenue generation. According to a Member State, cryptocurrency attacks allow the Democratic People's Republic of Korea to use the proceeds of their attacks

abroad more readily. To obfuscate their activities, attackers use a digital version of layering in which they create thousands of transactions in real time through one-time use cryptocurrency wallets. According to that Member State, stolen funds following one attack in 2018 were transferred through at least 5,000 separate transactions and further routed to multiple countries before eventual conversion to fiat currency, making it highly difficult to track the funds[118].

Another state involved in the practice is certainly Russia. It should be noted that Russia was not subject to widespread economic sanctions until 2014, when they were imposed after the annexation of Crimea. These were imposed by the European Union, and several were imposed by the US Treasury Department. As we have already had the opportunity to analyse, many areas in Russia are favourable to mining and mining activity has seen exponential growth in some locations, Siberia above all. Back in 2017, Putin had already stated that Russia would issue its own "CryptoRuble", with the same President warning citizens shortly before about the risks and dangers associated with cryptocurrencies in circulation. Furthermore, in 2019, the US announced sanctions against Evrofinance Mosnarbank, a Russian bank involved with the Venezuelan Petro. Petro's early adopters allegedly transferred funds to an account owned by the Venezuelan government at the aforementioned bank. In fact, Russia subsequently found it cheaper to create asset-backed cryptocurrencies than to create the crypto-ruble. Indeed, these should not be subject to fluctuations in exchange rates, fees and even trade restrictions[119].

As is well known, another troubled relationship is that between the US and Iran. US sanctions have affected the Middle Eastern state since 1979. As we have already discussed, the past decade has seen several events linked to the Joint Comprehensive Plan of Action, from the agreement and freezing of economic sanctions, to the withdrawal under the Trump administration with the imposition of a new package of sanctions that have once again hit the Iranian economy hard. Regarding cryptocurrencies, Iran's approach was initially very cautious. Subsequently, Iranian developers created a blockchain platform, IranRescueBit, with the aim of making donations via various cryptocurrencies, including Bitcoin, Ethereum and Litcoin, easier. This posed, in effect, a threat to circumvent and undermine the sanctions sought by Trump. This was followed, of course, by a November 2018 announcement by the US Treasury Department to watch out for cryptocurrency exchangers associated with Iranian cyber actors. The overview related to Iran appears complex, as on the one hand cryptocurrency mining was halted last June 2019, given the excessive strain inflicted on the state-subsidised electricity system, and on the other hand there was an announcement in July of the same year to create a nationwide cryptocurrency digital currency, useful for freeing frozen assets from local banks,

[118] United Nations Report of the Panel of Experts, S/2019/171. 2019. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/028/82/PDF/N1902882.pdf.

[119] Clautice, T. (2019). Nation State Involvement in Cryptocurrency and the Impact to Economic Sanctions.

supervised by the Central Bank of Iran and backed by gold reserves. The consequence of this was, rather pragmatically, the exclusion of all cryptocurrencies, which would not be recognised by the central bank as transactions, precisely to promote its own digital currency. Iran thus fits into the context of creating its own digital currency, in the wake of states such as Russia, China and Venezuela[120].

But how did this come about? Bitcoin has helped, in the recent past, to circumvent US sanctions imposed on Iran. Anonymous payments made with this cryptocurrency have allowed small and medium-sized companies to continue to conduct business, despite constant monitoring by the US. This was only curtailed in the 2019, when the central bank issued enhanced guidance on the prohibition of using global cryptocurrencies inside the country as a method of payment and four Iranian banks were willing to try towards the digital currency backed by gold, the PayMon. This seems to have potentially better prospects than the Venezuelan Petro as Iran enjoys greater stability and a more structured partnership with strong countries such as Russia and China. Armenia has also already entered the scene, signing a trilateral agreement with Russia and Iran with a view to blockchain cooperation[121]. Beyond the Iranian PayMon, what, here, it is interesting to underline, is how Iran has used the extraction of Bitcoin to evade US sanctions and export millions of barrels of oil through mining. Only in 2019 did Iran officially recognize cryptocurrency mining, even establishing a licensing regime that required miners to identify themselves, and the prospect of low-cost energy attracted a lot of internal investment, particularly from China. What can be called a paradox is that many of those who carry out these Bitcoin transactions and pay commissions to Iranian miners located in the United States, the very country that imposed the sanctions on Iran. Equally real is the risk from financial institutions offering cryptocurrency services. The risk of running into sanctions for being involved in operations that generate cryptocurrencies for Iranian miners is certainly relative, but not non-existent[122]. The percentage of Bitcoin mining in Iran has increased significantly in recent years, as can be seen from the figure below.

[120] Erdbrink, T. (2019, January 30). *How Bitcoin Could Help Iran Undermine U.S. Sanctions*. The New York Times. https://www.nytimes.com/2019/01/29/world/middleeast/bitcoin-iran-sanctions.html

[121] Mogielnicki, R. (2019, August 23). *Cryptocurrencies could help evade U.S. sanctions on Iran*. Axios. https://www.axios.com/cryptocurrencies-could-help-evade-us-sanctions-on-iran-c6a68e07-03c3-4b99-8dde-882d6f729130.html

[122] Robinson, T. (2021). *How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil*. Elliptic.co. Retrieved 19 September 2021, from https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions.

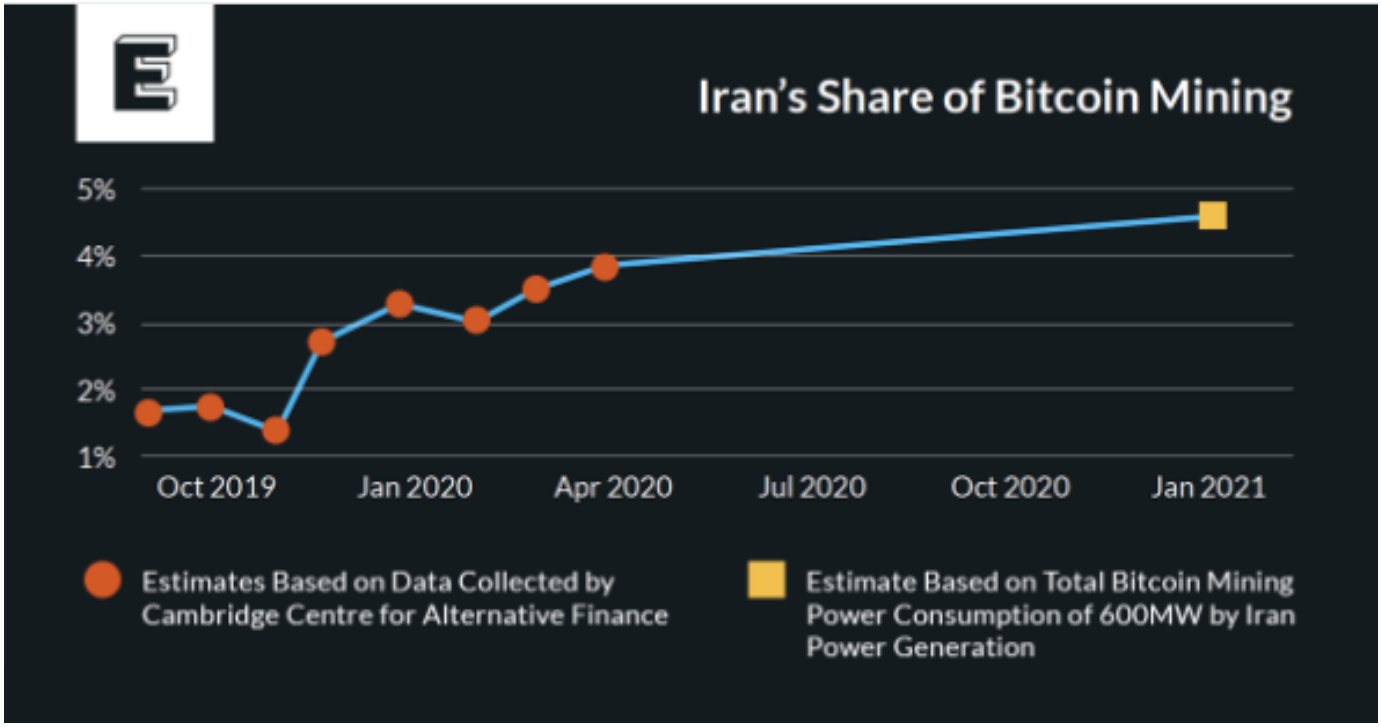


Figure 5.3 – Iran's Share of Bitcoin Mining

Source: Robinson, T. (2021). *How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil*. Elliptic.co. Retrieved 19 September 2021, from https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions.

About 4.5% of all Bitcoin mining takes place, therefore, in Iran. This translates into a turnover of $ 1 billion per year. The Middle Eastern state itself therefore recognized that this extraction benefits an economy severely hit by sanctions and that, moreover, it suffers from a scarce presence of cash but with a surplus for oil and natural gas. All ingredients that make the cryptocurrency recipe perfect for Iran[123].

A final state, which merits closer examination in this work, is Venezuela. Previously, we have already had the opportunity to address the developments in this country is the launch, by President Maduro, of the state cryptocurrency, the Petro. What is of interest here is to understand why this was launched, in addition to the economic motivations. In 2017 and 2018, there were numerous sanctions by the United States, and Nicolas Maduro was among them. Last August 2017, the United States, through an Executive Order, prohibited the Venezuelan government and state-owned oil companies from accessing the US financial market. In fact, this represented a strong impetus to Maduro's desire to create the Petro. The idea of being able to evade the US sanctions, combining a possible economic revival, replacing the Bolivar subject to hyperinflation, represented for Maduro a strong possibility also from a political point of view. Petro, as intended by the Venezuelan government, is a currency that is convertible into fiat currency, which can replace physical money by

[123] *Iran uses crypto mining to lessen impact of sanctions, study finds*. Reuters. (2021). Retrieved 19 September 2021, from https://www.reuters.com/technology/iran-uses-crypto-mining-lessen-impact-sanctions-study finds-2021-05-21/ .

purchasing national and international goods and services, as well as paying taxes and funding public services. The main goal is to sell Venezuelan oil to foreign countries without using US Dollars; indeed, the possibility of using cryptocurrency as a means of payment with OPEC Members was proposed and the Supreme Court of Justice of Venezuela legitimized the oil-backed cryptocurrency as a legal means of payment, and Turkey's foreign minister declared that Turkey recognized Petro as a legitimate means of payment[124].

What is of interest at this point in the analysis is to understand what strategies are adopted to circumvent sanctions. With the increase and continuation of economic sanctions, these practices have clearly become real strategies, even if they are not always officially decided upon, but rather represent a basket of opportunities to be used depending on the gravity of the situation or the type of sanction. As already mentioned, the first strategy is theft of cryptocurrencies from exchanges and individuals through cyber hacking. Russia and North Korea are known for their cyber capabilities. Cryptocurrency theft generally occurs in two forms. The first technique is direct theft of currency through computer hacking. The other illicit technique involves exploitation through hacking, then demanding cryptocurrency ransom to return the system to the status quo. The North Korean's collecting Bitcoin ransom payments from victims in the malware WannaCry attack that exploited vulnerabilities in the Windows operating system serves as a clear example of this method. The second strategy is related to cryptocurrency mining. As extensively discussed, this process requires numerous servers, a large power supply, substantial investments in technology, special weather conditions and low electricity costs. This pathway generates capital outside the global financial system as it relates to dollars vice a commodity, such as oil. "Russia, with its unique nexus of computer genius and money laundering expertise, looks set to become the new cryptocurrency world's Wild East. A third strategy, particularly pursued by Venezuela and Russia, but also by other states, as we have already seen, includes the creation of a national cryptocurrency. Venezuela clearly lacks the cyber capability and sophistication to take advantage of the current cryptocurrency market, and that's why the strategy has been creating a backed-state cryptocurrency. The fourth strategy entails coupling multiple states to a common cryptocurrency. This is best illustrated by the BRICS, who have recently entertained the idea of a supranational BRICSCoin to combat the dollar that is backed by their own basket of currencies and gold. This would certainly have negative consequences for the US, as linking Russia with China and India via a digital currency would make the application of economic sanctions much more difficult. A fifth strategy encourages a sanctioned state's population and business community to utilize all digital currencies freely. This hands-off approach by a state risk undermining its fiat currency. The greater the impact of the sanctions on the fiat currency, the greater the risk a government may be willing to take in cryptocurrency experimentation, especially if it translates to domestic economic stability. The

[124] Cozzi, F. (2020, July 1). *Will Blockchain Technologies Strengthen or Undermine the Effectiveness of Global Trade Control Regulations and Financial Sanctions?* De Gruyter. https://www.degruyter.com/document/doi/10.1515/gj-2019-0047/html

fundamental challenge for each of these cryptocurrency strategies used to avoid sanctions remains the conversion mechanism to fiat currencies. Major energy, commodity, and arms sales by sovereign states have yet to occur using only cryptocurrency. As blockchain proliferates in the global financial system, the likelihood of this first major transaction will increase. To be sure, financial institutions and governments the world over will take notice, but will they be ready to respond, or will they be forced to react?[125]

5.4 How to steam the illicit

The problem of sanctions evasion through cryptocurrencies has been explored and understood. The ability to utilise the properties of this instrument has led, in recent history, to numerous states evading economic sanctions, mainly by the United States and the United Nations, but also those imposed by the European Union. Curbing this type of offence is complicated. There are many actors involved, and it seems unlikely that there will be cooperation to ensure that transparency reigns in this type of operation, where the strategy adopted involves the transparency of certain entities or individuals, such as financial intermediaries when attempting to exchange cryptocurrencies for fiat currency. This is unlikely to happen because it would also damage the intermediaries economically by blocking an income stream that would be useful to the company, be it small, medium, or large. As we have seen, the strategies are different and, the capacity of some minds in operating cyber-attacks leads one to declare that, beyond all the properties and the ethical aspect that can be used by the actors involved in this process, sometimes not even a concerted effort of these is able to curb the capacity of some cyber criminals in operating attacks of a certain type and calibre.

In the current state of the phenomenon and its evolution, an important role is certainly played by OFAC, which, as we have already discussed, administers, and enforces various economic sanctions programmes against geographical regions, governments, groups, and individuals. To increase the risks to the cryptocurrency industry, OFAC has made it clear that preventing sanctions evasion through cryptocurrencies is a high priority for the agency, and it intends to use its sanctions authorities to counter the use of cryptocurrencies by sanctions targets and other malicious actors who abuse cryptocurrencies and emerging payment systems. The direction therefore appears to be first and foremost one of awareness and consciousness raising, which is made explicit by OFAC towards both users and the various agencies operating in the crypto-sector. If, therefore, on the one hand, in the embryonic phase of the phenomenon, it seemed too profitable to endorse this practice even for

[125] Konowicz, D. R. (2018). *The new game: cryptocurrency challenges US economic sanctions*. Naval War College Newport United States.

persons or entities that could have identified the illicit nature of the transaction, OFAC raises the stakes by hardening the possible countermoves once the fact is established[126].

The role of the FATF (Financial Action Task Force) should also be studied for the purposes of this analysis. Last March, in fact, the intergovernmental organisation founded in 1989 in Paris at the instigation of the G7, published its new draft guidance on virtual assets (VAs) and virtual asset service providers (VASPs), with the aim of finalising the proposal by the end of 2021. The draft builds on the guidance on VAs and VASPs published by the same intergovernmental organisation in June 2019. It established the need for providers of these services to undertake several obligations in relation to anti-money laundering and combating the financing of terrorism, such as the collection of Customer Due Diligence (CDD) or Know Your Customer (KYC). The latest guidance, in fact, aims to implement the previous one and solve some of its problems also in relation to the definition of what can be considered as a VA or VASP. It is reaffirmed that "stable coins" are also subject to the AML/CFT rules, being, in fact, equivalent to fiat currencies. The interpretation of VAs and VASPs themselves must be broad, to accommodate different technological advances and business models. The guidance also deals with non-fungible tokens (NFTs). While the previous proposal stated that the standards only covered virtual assets that were considered fungible, i.e., those that were not unique and immediately replaceable, the new guide is implemented and modified in this sense, embracing also Non-Fungible Tokens[127]. This requires cryptocurrency exchanges, wallet providers and institutions involved in the industry to share the identities of users who are involved in any transfer of virtual assets. However, most countries have not yet implemented the FATF requirements, including the 'travel rule'. The draft guidance, which consists of a hundred pages and is divided into several sections, has been implemented by 58 of the 128 reporting jurisdictions. "Lack of regulation or implementation of regulation in jurisdictions may allow continued misuse of virtual assets through jurisdictional arbitrage," the FATF said during the plenary session. The FATF in its latest report highlighted the need for all jurisdictions to implement the revised standards as quickly as possible. The report also identified potential future FATF actions to prevent the misuse of virtual

[126] Mosman, B., Mortlock, D., Gray, E. P., Giancarlo, C. J., & Hall, S. (2021, August 17). *OFAC Sanctions Considerations for the Crypto Sector*. Willkie Farr & Gallagher LLP. Retrieved September 15, 2021, from https://www.willkie.com/-/media/files/publications/2021/08/ofacsanctionsconsiderationsforthecryptosector.pdf.

[127] Fatf-gafi.org. (2021). Retrieved 20 September 2021, from https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf.

assets for criminal activities, including an emphasis on actions to help mitigate the risk of the use of virtual assets linked to ransomware[128].

As we have been able to understand and analyse, due to the massive development in the use of cryptocurrencies and then of actors involved in the exchange of virtual currencies, the key word in recent times has become regulation. Various actors, state, intra-state, and inter-state have been or are in the process of regulating the sector, both to prevent the illicit use of cryptocurrencies and to take advantage of it. This regulation, however, which is carried out at different levels and in a variety of ways, appears far from being totally effective, especially in combating anti-money laundering and combating financial terrorism and, partially, also about the evasion of sanctions through cryptocurrencies. This is because the actors that have intervened over the years, including international organisations, have succeeded to a large extent in curbing the various illicit phenomena associated with the use of cryptocurrencies, but have always turned out to be state or regional actors. Real regulation should perhaps take place through an institution that truly allows for the inclusion of most states (and thus indirectly includes companies and exchanges) and that can provide a global and broad framework.

Logically, both international organisations and states found themselves faced with a phenomenon that was on the rise and developing without having a legal structure that could be adequate to manage it. It should also be stressed that the perspective of many actors has been that of "wait and see", also to avoid interrupting a revolution without waiting for possible developments that could also benefit the governments themselves. The biggest concern, over time, has been about the impact that cryptocurrencies have on the ability of national governments to generate revenue and on the ability of banks to implement monetary policy choices should virtual currencies become more widely used than fiat currencies. Hence the need for regulation. As has already been pointed out extensively throughout this paper, it is the borderless nature of cryptocurrencies that makes regulation complicated and, more generally, we return to the dilemma already presented: how to govern something born not to be governed?[129]

To date, the legal status of cryptocurrencies, as partially analysed, varies from country to country. Several countries have frameworks in place to give a legal boundary to the use of cryptocurrencies. Among the regulatory frameworks not analysed in depth but worth mentioning is the case of Switzerland. Switzerland's political system provides citizens with plenty of space and opportunities to make changes to existing laws.

---

[128] *Most nations yet to implement FATF's anti-money laundering standards for crypto*. mint. (2021). Retrieved 20 September 2021, from https://www.livemint.com/news/india/most-nations-yet-to-implement-fatf-s-anti-money-laundering-standards-for-crypto-11624678189336.html.

[129] Jacobs, G. (2018). Cryptocurrencies & the challenge of global governance. *Cadmus*, *3*(4), 109-123.

Direct democracy is, as is well known, a strong feature in the country[130]. In 2018, a partnership for the improvement of blockchain was created (Swiss Federation of Blockchain) and in the same country, people have already started talking about "Crypto Valley", in the wake of the US Silicon Valley. Returning to the regulatory issue, Switzerland has some of the most stringent anti-money laundering and know-your-customer policies in place. The Financial Market Supervisory Authority (FINMA), the body responsible for financial regulation in the country, has implemented several legislative changes over the years to incorporate the FATF recommendations, such as the "Travel Rule" mentioned above. The presence in Basel of the Bank of International Settlements and the Basel Committee (which operates under the auspices of the BIS) obviously makes Switzerland more sensitive to changes and developments in the crypto sector. In any case, exchanges are legal if they are authorised by FINMA, although they have more stringent rules, but also because they have more specific regulations, regarding VASPs. Since 2019, FINMA has also licensed two financial institutions to carry out cryptocurrency trading and custody activities. Mining is also permitted in Switzerland and there are very specific ICO (Initial Coin Offerings) regulations. By virtue of the country's concentration of wealth and several other reasons, Switzerland is considered an ideal country when it comes to ICOs and, after the boom that took place between 2016 and 2017, a number of relevant regulations were developed in 2018. Pioneering also for many other states, such as the US, Switzerland, and in particular FINMA, has adopted the "same deal, same rules" approach by drafting specific guidelines regarding ICOs. Returning to the 'Crypto Valley', the phenomenon is quite recent: in 2020, residents of the canton of Zug were informed of the possibility to pay taxes in Bitcoin up to 100,000 francs. The Federal Tax Administration (FTA), which oversees tax collection, considers cryptocurrencies such as Bitcoin, Ethereum etc. to be real assets and are therefore covered by Swiss wealth tax. In conclusion, there is of course the "Blockchain Act", a set of laws passed in 2020, with the aim of looking to the future with the inclusion of DLT[131].

[130] Jackson, O. (2018). US or Swiss approach for EU crypto regulation?. *International Financial Law Review*.

[131] Dutta, S. (2021). *Switzerland Crypto Regulations: KYC, Taxes & FINMA*. Coinfirm.com. Retrieved 21 September 2021, from https://www.coinfirm.com/blog/switzerland-crypto-regulations/.

CONCLUSIONS

In the course of the work, it was necessary to clarify the basics, study and deepen them, and then move with an interdisciplinary approach trying to give answers to the phenomenon object of the thesis. The evasion of penalties through cryptocurrencies is a phenomenon that is as stimulating as it is recent. The cases have been explained and examined in depth, as well as the methods, strategies, and objectives, more or less veiled, behind the implementation of this offence. On a geopolitical level, it is certainly interesting to note how numerous states violate US sanctions also and above all to try to undermine its hegemony. Undoubtedly, actors such as Iran and Venezuela have suffered a strong backlash at the domestic economic level after the US sanctions, mainly due to the exclusion, as seen, from the SWIFT system and also from the strong western relations of the US. This has changed under the Trump administration, with the West, and in particular the European Union, wanting to maintain relations with the Middle Eastern state rather than endorse the sanctions issued by the US at the time. More generally, always from the geopolitical aspect, what we have tried to demonstrate is the new centrality and importance of a spatial dimension that is not physical, but virtual. We often speak of the massive cybernetic investments and of the new wars that will take place in forms that are unknown but far from what most of the world population is accustomed to understanding, what we have tried to deepen and understand in this work is how in the virtual space revolutions are taking place that are able to have strong repercussions and generate strong concerns both under the political and economic aspects. Cryptocurrencies are a phenomenon born, objectively, from the lack of trust placed in international financial institutions. What is also true is that perhaps the same institutions, national and international, did not expect an evolution of this magnitude, in so few years and have been forced to make choices. Some States, as we have had the opportunity to note and deepen, have tried to appropriate this phenomenon also to put an end to long-term economic crises, trusting in the response of their own governed, and this does not depend on being sanctioned by the United States, the UN, or the EU. Cases such as those in El Salvador are certainly a warning to the international community, as are the various episodes in numerous African states, Spain, and Cyprus, where over the years demand for Bitcoin and other cryptocurrencies has increased precisely because of unfavourable political and economic circumstances, considering virtual currencies a safe haven. The use of the innovative tool of cryptocurrencies to circumvent economic sanctions is certainly fascinating in its study. States deciding to make strong choices such as thinking about creating a national cryptocurrency, or even doing so (Venezuelan Petro), suggests that the current economic system is pushing some state economies to their limits. On the other hand, there is also a strong desire to exploit this phenomenon to bring about a political and economic revolution and to undermine the United States as the world's leading economic power, discouraging the use of the dollar and replacing it with a 'regional' cryptocurrency, in line with the BRICScoin idea.

At the end of this work, there are many questions that struggle to be answered. Are we really facing a revolution capable of creating enormous social progress and, above all, allowing for the first time in history to have a global currency? What are the geopolitical dynamics that follow? What considerations is it possible to make if this could happen? What international organisation would be able to bring about, even at a legal level, this kind of revolution and then implement its effective management, trying to limit financial speculation and the influence of the rich within the markets? What aspects can be improved in the use of cryptocurrencies thanks to the numerous institutional forums? What room for improvement does blockchain technology have and how much can actors at all levels benefit from it? Personally, the aim of this paper has never been to answer the first question, because even attempting to do so would require economic skills that do not belong to me. The focus on which I wanted to dwell was the understanding of the political and geopolitical dynamics following the evasion of the sanctions and, how, in virtue of a fact that has happened, it is possible to contain it or put an end to it. Certainly, in my view, the biggest question mark concerns global regulation, which now seems necessary. Global regulation should not be aimed at incorporation, because cryptocurrencies are born precisely to be ungoverned, and cases such as that of Venezuela distort their peculiarities and create a digital currency with monitoring, surveillance and control institutions that are state-owned. So, we are talking about a state digital currency, not a cryptocurrency. I believe that the various fora, both national and international, realise that it is impossible to take this revolution into their own hands, because only the attempt to move in this direction would perhaps lead to the failure of the current system, but leave room for a new system that could impose itself with equal and similar characteristics. I believe that the cryptocurrency phenomenon is founded on fundamentals that should be "listened to" and not silenced. Incorporating the system in its integrity is something that is simply incompatible. At the same time, there is a need, as already mentioned, for regulation that is global. Although, as we have seen, international organisations and states have dwelt extensively on directives and laws against money laundering, terrorist financing and other criminal uses of cryptocurrencies, the most recent and, certainly, the least known is that of economic sanctions evasion through cryptocurrencies. In fact, the scope is much broader if the audience is extended not only to states but also to companies and individuals, given the explosion of targeted sanctions since the end of the Cold War. For all these reasons, I maintain that a global regulation must also include this type of crime, because this is what we are talking about. Regarding the most appropriate bodies, there is no doubt that the United Nations is the international organisation that represents the most states globally. The World Trade Organisation, on the other hand, although it has fewer member states (164 against 193), has more democratic characteristics. As is well known, all member states are represented in both the plenary body (the Ministerial Conference) and the executive body (the General Council). It should also be noted that the WTO has had cooperation agreements with both Bretton Woods institutions (IMF and WB) since 1996. However, although the young international organisation deals with the goods sector in the narrow sense, and the issue of currency circulation is far from its remit, other features make it abstractly more suitable to deal with such an issue. What is, however, essential in the

perspective of regulation is to reach as many states as possible by providing incentives to ensure that acceptance is massive and not confined to a few actors. In conclusion, the real revolution that has already been adopted and that has the most immediate margins for incorporation is certainly related to the blockchain. By analysing the blockchain as a method and as a technological process, and unbundling it from the use made of cryptocurrencies, many states and international organisations are implementing choices and policies capable of simplifying daily operations in various sectors through this technology, a revolution in processes, both state and non-state, capable of making the relationship between state and citizen more transparent.

REFERENCES

Aarvik, P. (2020). Blockchain as an anti-corruption tool: Case examples and introduction to the technology. *U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute (U4 Issue 2020: 7)*.

Adrian, T., & Weeks-Brown, R. (2021). *Cryptoassets as National Currency? A Step Too Far*. IMFBlog. Retrieved 9 September 2021, from https://blogs.imf.org/2021/07/26/cryptoassets-as-national-currency-a-step-too-far/.

Alharby, M., & Van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. *arXiv preprint arXiv:1710.06372*.

Anthony, I. (2002). Sanctions applied by the European Union and the United Nations. *SIPRI YEARBOOK*, 203-230.

Antonakakis, N., Chatziantoniou, I., & Gabauer, D. (2019). Cryptocurrency market contagion: Market uncertainty, market complexity, and dynamic portfolios. *Journal of International Financial Markets, Institutions and Money, 61*, 37-51.

Árnason, S. L. (2015). *Cryptocurrency and Bitcoin. A possible foundation of future currency: why it has value, what is its history and its future outlook* (Doctoral dissertation).

Bakis, H. (2013). Fragilité du géocyberespace à l'heure des conflits cybernétiques. *Netcom. Réseaux, communication et territoires*, (27-3/4), 293-308.

Ballis, A., & Drakos, K. (2021). The explosion in cryptocurrencies: a black hole analogy. *Financial Innovation*, *7*(1), 1-8.

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, *19*(10), 1.

Betro N. (2021), "Pechino tra criptovalute e yuan digitale", Il Caffè Geopolitico, Internet: https://ilcaffegeopolitico.net/525510/pechino-tra-criptovalute-e-yuan-digitale (viewed on 30/07/2021).

Biersteker, T. J., Eckert, S. E., & Tourinho, M. (2016). *Targeted sanctions: The impacts and effectiveness of united nations action*. Cambridge University Press.

Bootwala, M. (2020). The iran problem: An evaluation of US sanctions on iran and global reactions. *Georgetown Journal of International Affairs, 21*, 136-141. https://doi.org/10.1353/gia.2020.0009

Brezo, F., & Bringas, P. G. (2012). Issues and risks associated with cryptocurrencies such as Bitcoin.

Brown, G., & Whittle, R. (2020). *Algorithms, blockchain & cryptocurrency: Implications for the future of the workplace*. Emerald Group Publishing.

Burlacu, N. V. (2021). Cryptocurrencies, Money of the Future or the Future of Money. *EIRP Proceedings, 16*(1).

Campbell-Verduyn, M. (2017). *Bitcoin and beyond: cryptocurrencies, blockchains and global governance*. Taylor & Francis.

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law, and Social Change, 69*(2), 283-305. https://doi.org/10.1007/s10611-017-9756-5

Carisch E., Rickard-Martin L., Meister, S. R. (2017), *The Evolution of UN Sanctions From a Tool of Warfare to a Tool of Peace, Security and Human Rights*. Springer International Publishing AG.

Cavalieri E. (2019), Geopolitica e mondo cibernetico: incontro tra passato e futuro, dicembre, Roma: Trinità dei Monti think tank.

CGC (2019), "Cryptocurrencies and the Future of Money", *Center for the Governance of Change*, Madrid: IE University.

Chohan, U. W. (2018). Cryptocurrencies as asset-backed instruments: The Venezuelan Petro. *Available at SSRN 3119606*.

Clautice, T. (2019). Nation State Involvement in Cryptocurrency and the Impact to Economic Sanctions.

ComplyAdvantage. (2021). *A New Sanctions Regime and a Spotlight on Crypto*. Retrieved 18 September 2021, from https://complyadvantage.com/blog/a-new-sanctions-regime-and-a-spotlight-on-crypto/ .

Cozzi, F. (2020, July 1). *Will Blockchain Technologies Strengthen or Undermine the Effectiveness of Global Trade Control Regulations and Financial Sanctions?* De Gruyter. https://www.degruyter.com/document/doi/10.1515/gj-2019-0047/html

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.

Current Trends and Ofac's Best Practices for Compliance - Association of Certified Sanctions Specialists. Association of Certified Sanctions Specialists. (2021). Retrieved 19 September 2021, from https://sanctionsassociation.org/sanctions-in-the-cryptocurrency-space-current-trends-and-ofacs-best-practices-for-compliance/.

Dabrowski, M., & Janikowski, L. (2018). Virtual currencies and central banks monetary policy: challenges ahead. *Monetary Dialogue. Policy Department for Economic, Scientific and Quality of Life Policies. European Parliament. Brussels*.

DeVries, P. D. (2016). An analysis of cryptocurrency, bitcoin, and the future. *International Journal of Business Management and Commerce*, *1*(2), 1-9.

Diariooficial.gob.sv. (2021). Viewed on 9 September 2021, from https://www.diariooficial.gob.sv/diarios/do-2021/06-junio/09-06-2021.pdf.

Dilek, Ş., & Furuncu, Y. (2019). Bitcoin mining and its environmental effects. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi*, *33*(1), 91-106.

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*. Rand Corporation.

Dorfler, T. (2019). *Security council sanctions governance: The power and limits of rules* (1st ed.). Routledge. https://doi.org/10.4324/9780429442322

Dow, S. (2019). Monetary reform, central banks, and digital currencies. *International Journal of Political Economy*, *48*(2), 153-173. https://doi.org/10.1080/08911916.2019.1624317

Dutta, S. (2021). *Switzerland Crypto Regulations: KYC, Taxes & FINMA*. Coinfirm.com. Retrieved 21 September 2021, from https://www.coinfirm.com/blog/switzerland-crypto-regulations/.

ElBahrawy, A., Alessandretti, L., Kandler, A., Pastor-Satorras, R., & Baronchelli, A. (2017). Evolutionary dynamics of the cryptocurrency market. *Royal Society open science*, *4*(11), 170623.

Erdbrink, T. (2019, January 30). *How Bitcoin Could Help Iran Undermine U.S. Sanctions*. The New York Times. https://www.nytimes.com/2019/01/29/world/middleeast/bitcoin-iran-sanctions.html

European Commission and European Central Bank (2021), *Joint statement by the European Commission and the European Central Bank on their cooperation on a digital euro*, Internet: https://ec.europa.eu/info/files/210119-ec-ecb-joint-statement-digital-euro_en (viewed on 16/09/2021)

European Union (2021), "Restrictive measures following the 2020 Belarus presidential elections", *Sanctions: how and when the EU adopts restrictive measures*, Internet: https://www.consilium.europa.eu/it/policies/sanctions/restrictive-measures-following-the-2020-belarus-presidential-elections/ (viewed on 21/08/2021).

Fantacci, L., & Gobbi, L. (2021). Stablecoins, Central Bank Digital Currencies and US Dollar Hegemony. *Accounting, Economics, and Law: A Convivium*.

Farrall, J. M. (2007;2009;). *United nations sanctions and the rule of law*. Cambridge University Press. https://doi.org/10.1017/CBO9780511494352

Fatf-gafi.org. (2021). Retrieved 20 September 2021, from https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf.

FAUZI, M. A., PAIMAN, N., & OTHMAN, Z. (2020). Bitcoin and cryptocurrency: Challenges, opportunities and future works. *The Journal of Asian Finance, Economics, and Business*, *7*(8), 695-704.

Fidler, D. P. (2016). Cyberspace, terrorism and international law. *Journal of Conflict and Security Law*, *21*(3), 475-493.

Fitzpatrick, M. (2017). Assessing the JCPOA. *Adelphi Series*, *57*(466-467), 19-60.

Fleming. S., Pickford, S. (2021), "Digital currencies: Economic and geopolitical challenges", Chatham House, Internet: https://www.chathamhouse.org/2021/01/digital-currencies-economic-and-geopolitical-challenges , (viewed on 03/09/21)

Frolov, A. V. (2021). The Biden Administration and the Iran Nuclear Deal. *USA & Canada: ekonomika, politika, kultura*, (7), 48-62.

Gibbons F., Garfield R. (1999), "The impact of economic sanctions on health and human rights in Haiti, 1991-1994, in *American Journal of public health (1971)*, Volume 89, Issue 10, pp. 1499-1504.

Girasa, R. (2018). *Regulation of cryptocurrencies and blockchain technologies: national and international perspectives*. Springer.

Giumelli, F. (2011). *Coercing, constraining and signalling: Explaining UN and EU sanctions after the cold war*. ECPR press.

Giumelli, F. (2013). How EU sanctions work: A new narrative. *Chaillot Papers (Paris), 129, May 2013*

Giumelli, F. (2016). *The success of sanctions: lessons learned from the EU experience*. Routledge.

Giumelli, F., Hoffmann, F., & Książczaková, A. (2021). The when, what, where and why of European Union sanctions. *European Security*, *30*(1), 1-23.

Goodkind, A. L., Jones, B. A., & Berrens, R. P. (2020). Cryptodamages: Monetary value estimates of the air pollution and human health impacts of cryptocurrency mining. *Energy Research & Social Science*, *59*, 101281.

Gordon, J. (2010). *Invisible war: the United States and the Iraq sanctions*. Harvard University Press.

Gordon, R., Smyth, M., & Cornell, T. (2019). *Sanctions Law*. Bloomsbury Publishing.

Grech, A., & Camilleri, A. F. (2017). *Blockchain in education*. Luxembourg: Publications Office of the European Union.

Group, G. (2021). *Sanctions 2021 | Rising Risk: Recent Developments in Cryptocurrency Sanctions and Enforcement | ICLG*. International Comparative Legal Guides International Business Reports. Retrieved 16 September 2021, from https://iclg.com/practice-areas/sanctions/3-rising-risk-recent-developments-in-cryptocurrency-sanctions-and-enforcement.

Gururaj, H. L., Manoj Athreya, A., Kumar, A. A., Holla, A. M., Nagarajath, S. M., & Ravi Kumar, V. (2020). Blockchain: A new era of technology. *Cryptocurrencies and Blockchain Technology Applications*, 1-24.

Hacker, P., & Thomale, C. (2018). Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law. *European Company and Financial Law Review*, *15*(4), 645-696.

Hagen, J. (2021). *6AMLD the Five Key Changes*. Skillcast.com. Retrieved 16 September 2021, from https://www.skillcast.com/blog/6amld-key-changes.

Hanke, S., Hanlon, N., & Chakravarthi, M. (2021). *Bukele's Bitcoin Blunder* (No. 185). The Johns Hopkins Institute for Applied Economics, Global Health, and the Study of Business Enterprise.

Hegadekatti, K. (2016). Governance and geopolitics in the age of blockchains and cryptocurrencies. *Available at SSRN 2889314*.

Herr, T. (2020). Four Myths about the Cloud: The Geopolitics of Cloud Computing.

Hewa, T., Ylianttila, M., & Liyanage, M. (2020). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, 102857.

Hixson W., L. (2021), "Biden Following Trump Policy on Iran, Nuclear Deal, *The Washington report on Middle East affairs*, Volume 40, Issue 3, pp. 54-55.

Holman, D., & Stettner, B. (2018). Anti-Money Laundering Regulation of Cryptocurrency: US and Global Approaches. *Електронний ресурс]/D. Holman, S. Barbara//Allen & Overy LLP.–2018.–Режим доступу до ресурсу: http://www.allenovery.com/publications/engb/Documents/AML18_AllenOvery. pdf*.

Houben, R., & Snyers, A. (2018). Cryptocurrencies and blockchain. *Legal context and implications for financial crime, money laundering and tax evasion*.

Houben, R., & Snyers, A. (2020). *Crypto-assets: Key developments, regulatory concerns and responses*.

Hsieh, Y., Vergne, J., & Wang, S. (2017). The internal and external governance of blockchain-based organizations: Evidence from cryptocurrencies. (pp. 48-68)https://doi.org/10.4324/9781315211909

Houben, R., & Snyers, A. (2020). *Crypto-assets: Key developments, regulatory concerns and responses.*

IlPost (2021), "Perché l'industria dei bitcoin sta lasciando la Cina", IlPost, Internet: https://www.ilpost.it/2021/07/04/migrazione-miner-bitcoin-cina-texas/ (viewed on 20/07/21)

Iran uses crypto mining to lessen impact of sanctions, study finds. Reuters. (2021). Retrieved 19 September 2021, from https://www.reuters.com/technology/iran-uses-crypto-mining-lessen-impact-sanctions-study finds-2021-05-21/ .

Jackson, O. (2018). US or Swiss approach for EU crypto regulation?. *International Financial Law Review.*

Jacobs, G. (2018). Cryptocurrencies & the challenge of global governance. *Cadmus (Trieste, Italy), 3*(4), 109-123.

Jiang, B., & Ormeling, F. (2000). Mapping cyberspace: Visualizing, analysing and exploring virtual worlds. *Cartographic Journal, 37*(2), 117-122. https://doi.org/10.1179/caj.2000.37.2.117.

Jones E. (2020), "A Quick History of Cryptocurrency in China", CryptoVantage, Internet: https://www.cryptovantage.com/guides/history-of-crypto-in-china/ (viewed on 04/09/21)

Jovanić, T. (2020). An Overview of Regulatory Strategies on Crypto-Asset Regulation-Challenges for Financial Regulators in the Western Balkans. In *Tatjana Jovanić, An Overview of Regulatory Strategies on Crypto-Asset Regulation-Challenges for Financial Regulators in the Western Balkans, in: EU Financial Regulation and Markets-Beyond Fragmentation and Differentiation (Eds. I. Bajakić, M. Božina Beroš), Conference Proceedings, Zagreb*.

Kadir, N. K., Judhariksawan, J., & Maskun, M. (2019). Terrorism and cyberspace: A phenomenon of cyber-terrorism as transnational crimes. *FIAT JUSTISIA: Jurnal Ilmu Hukum*, *13*(4), 333-344.

KAEMPFER, W. H., & MOFFETT, M. H. (1988). impact of anti-apartheid sanctions on south africa: Some trade and financial evidence. *Contemporary Economic Policy, 6*(4), 118-129. https://doi.org/10.1111/j.1465-7287.1988.tb00551.x

Kaiser, B., Jurado, M., & Ledger, A. (2018). The looming threat of China: An analysis of Chinese influence on Bitcoin. *arXiv preprint arXiv:1810.02466.*

Kalehsar, O. S. (2020). The geopolitics of U.S. energy sanctions against iran. *Middle East Policy*, *27*(2), 108-119. https://doi.org/10.1111/mepo.12498

Kapsis, I. (2020). Blockchain and cryptocurrencies: essential tools in a two-tier financial system. *Capital Markets Law Journal*.

Kaur, A., Nayyar, A., & Singh, P. (2020). Blockchain: A path to the future. *Cryptocurrencies and Blockchain Technology Applications*, 25-42.

Kelly, B. (2014). *The bitcoin big bang: How alternative currencies are about to change the world* (1st ed.). Wiley.

Konoth, R. K., Vineti, E., Moonsamy, V., Lindorfer, M., Kruegel, C., Bos, H., & Vigna, G. (2018, October). Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1714-1730).

Konowicz, D. R. (2018). *The new game: cryptocurrency challenges US economic sanctions*. Naval War College Newport United States.

Korosteleva, E. A. (2016). The european union and belarus: Democracy promotion by technocratic means? *Democratization*, *23*(4), 678-698. https://doi.org/10.1080/13510347.2015.1005009

Lamanna A. (2016), "Revival etnico 2.0. Indipendentismi nel cyberspazio", *Alpha Cyber Security Research Project*, settembre, Roma: The Alpha Institute of Geopolitics and Intelligence.

Lamanna A. (2016) "Per una geopolitica del cyberspazio", *Alpha Cyber Security Research Projec*t, marzo, Roma: The Alpha Institute of Geopolitics and Intelligence.

Lay S., Pascarella M. (2016), "L'utilizzo del cyberspazio da parte del terrorismo islamico", *Alpha Cyber Security Research Projec*t, marzo, Roma: The Alpha Institute of Geopolitics and Intelligence.

Lie T. (1948), "Trygve Lie Appraises the Future of the U.N.", *New York Times*, May 9, p. 175, 182, 184.

Macfarlane, E. K. (2021). strengthening sanctions: Solutions to curtail the evasion of international economic sanctions through the use of cryptocurrency. *Michigan Journal of International Law, 42*(1), 199-229.

Makridakis, S., & Christodoulou, K. (2019). Blockchain: Current challenges and future prospects/applications. *Future Internet*, *11*(12), 258.

Martino, L. (2018). La quinta dimensione della conflittualità. L'ascesa del cyberspazio ei suoi effetti sulla politica internazionale. *Politica & Società, 7*(1), 61-76.

Matharu, A. (2018), *Understanding cryptocurrencies: the money of the future*. New York: Business Expert Press.

Mogielnicki, R. (2019, August 23). *Cryptocurrencies could help evade U.S. sanctions on Iran*. Axios. https://www.axios.com/cryptocurrencies-could-help-evade-us-sanctions-on-iran-c6a68e07-03c3-4b99-8dde-882d6f729130.html

Mosman, B., Mortlock, D., Gray, E. P., Giancarlo, C. J., & Hall, S. (2021, August 17). *OFAC Sanctions Considerations for the Crypto Sector*. Willkie Farr & Gallagher LLP. Retrieved September 15, 2021, from https://www.willkie.com/-/media/files/publications/2021/08/ofacsanctionsconsiderationsforthecryptosector.pdf

Most nations yet to implement FATF's anti-money laundering standards for crypto. mint. (2021). Retrieved 20 September 2021, from https://www.livemint.com/news/india/most-nations-yet-to-implement-fatf-s-anti-money-laundering-standards-for-crypto-11624678189336.html.

Nagarajan, M. (2018). An Analysis of Cryptocurrency Governance.

Nizhnikau, R. (2020). Playing the enemies: Belarus finds in between EU and Russian sanctions regimes. *Revista CIDOB d'Afers Internacionals*, Issue 125, 113-137.

Nugent, C. (2021). El salvador goes bitcoin. *Time (Chicago, Ill.), 197*(23/24), 18.

Odayar, T. (2021). Alternating current: El salvador to harness volcanic energy for bitcoin mining. *Power Finance & Risk.*

Office of Foreign Assets Control - Sanctions Programs and Information. U.S. Department of the Treasury. (2021). Viewed on 18 September 2021, from https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information .

Osula, A. M., & Rõigas, H. (Eds.). (2016). *International cyber norms: Legal, policy & industry perspectives*. NATO Cooperative Cyber Defence Centre of Excellence.

Panda, S. K., Elngar, A. A., Balas, V. E., & Kayed, M. (Eds.). (2020). *Bitcoin and Blockchain: History and Current Applications*. CRC Press.

Pascual, C. (2015). The new geopolitics of energy. *The Center on Global Energy Policy. Columbia University in the City of New York School of International and Public Affairs (SIPA)*.

Pernice, I. G. A., & Scott, B. (2021). Cryptocurrency. *Internet Policy Review, Glossary of decentralised technosocial systems, 10*(2).

Plassaras, N. A. (2013). Regulating digital currencies: bringing Bitcoin within the reach of IMF. *Chi. J. Int'l L., 14*, 377.

Portela, C. (2011). The european union and belarus: Sanctions and partnership? *Comparative European Politics (Houndmills, Basingstoke, England)*, *9*(4-5), 486-505. https://doi.org/10.1057/cep.2011.13

Portela, C. (2012). *European union sanctions and foreign policy: When and why do they work?*https://doi.org/10.4324/9780203847510

Popa, I. F. (2013). EU Cyberspace Governance: Which Way Forward. *Res. & Sci. Today*, *5*, 115.

Radu, R. (2014). Power technology and powerful technologies: global governmentality and security in the cyberspace. In *Cyberspace and International Relations* (pp. 3-20). Springer, Berlin, Heidelberg.

Ramamurthy, B. (2020). *Blockchain in action*. Manning Publications.

Richter, C., Kraus, S., & Bouncken, R. B. (2015). Virtual currencies like Bitcoin as a paradigm shift in the field of transactions. *International Business & Economics Research Journal (IBER)*, *14*(4), 575-586.

Robinson, T. (2021). *How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil*. Elliptic.co. Retrieved 19 September 2021, from https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions.

Roche, E. M., & Blaine, M. J. (2013). Convention internationale sur l'utilisation pacifique du cyberespace. *Netcom. Réseaux, communication et territoires*, (27-3/4), 309-330.

Sanguin, A. L. (2014). Fine della geografia o rivincita della geografia. *Le societa umane in un mondo liscio, un mondo „puntuto" o un mondo piatto//Bollettino della Societa Geografica Italiana. Serie XIII*, *7*, 445-460.

Schjolberg, S. (2007). Terrorism in Cyberspace-Myth or reality.

Sedgwick K. (2018), "Eight historic Bitcoin transactions", Bitcoin.com, Internet: https://news.bitcoin.com/eight-historic-bitcoin-transactions/ , (viewed on 28/08/2021)

Shilo, P., & Rosenblum, T. President Biden Has Five Options for Future Negotiations with Iran.

Silingardi S. (2020), *Le sanzioni unilaterali e le sanzioni con applicazione extraterritoriale nel diritto internazionale*. Milano: Giuffrè Francis Lefebvre.

Spithoven, A. (2019). Theory and reality of cryptocurrency governance. *Journal of Economic Issues*, Volume 53, Issue 2, 385-393.

Sposini A., Patriarca M. (2021). "La geografia del cyberspazio Cavi sottomarini, Data Center e Cloud Service Provider: tra connettivita' e competizione", *Geopolitical Brief*, n.18, pp. 1-23.

Sponeck, G. H. C., & von Sponeck, H. C. (2006). *A different kind of war: the UN sanctions regime in Iraq*. Berghahn Books.

Stephanides, J., Cortright, D., Lopez, G. A., Bondi, L., Biersteker, T. J., Brzoska, M., ... & Rogers, A. S. (2002). *Smart sanctions: targeting economic statecraft*. Rowman & Littlefield.

The Value Trend (2021), "The Geopolitics of Bitcoin", Seeking Alpha, Internet: https://seekingalpha.com/article/4428654-the-geopolitics-of-bitcoin-btc , (viewed on 03/09/21)

Titarenko, L. (2018). Belarus and the European Union. From confrontation to the dialogue. *CSE Working Papers 18| 01: febbraio 2018*.

Trump, B. D., Wells, E., Trump, J., & Linkov, I. (2018). Cryptocurrency: governance for what was meant to be ungovernable. *Environment Systems and Decisions*, *38*(3), 426-430.

United Nations Report of the Panel of Experts, S/2019/171. 2019. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/028/82/PDF/N1902882.pdf.

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(11), 2266-2277.

World Bank (2018), *Cryptocurrencies and Blockchain*, World Bank Europe and Central Asia Economic Update, Office of the Chief Economist, May, Washington.

Xie, R. (2019). Why china had to ban cryptocurrency but the u.s. did not: comparative analysis of regulations on crypto-markets between the u.s. and china. *Washington University Global Studies Law Review, 18(2)*, 457-492.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

ABSTRACT

The final work aims to analyse the complex and recent mechanism of economic sanctions evasion through cryptocurrencies by different actors. In order to proceed to a detailed analysis of the phenomenon and with the aim of providing answers to what could be the actions to be taken in order to limit or cancel it, it was necessary to study all the elements involved: firstly, the stage of reference, namely cyberspace; secondly, the institution of sanctions and, subsequently, cryptocurrencies, the instrument through which sanctions are circumvented. Finally, using an interdisciplinary approach, the various topics were linked and analysed in depth to explain the phenomenon.

MAPPING AN INVISIBLE BOUNDARY: THE GEOPOLITICS OF DIGITAL SPACE

Cyberspace is a term that is being used more and more and is known by more and more people, since the same use is now made on a daily basis in most parts of the planet. Defined as a computer-generated landscape, it is able to connect people, computers, and various sources of information in the world through which one can navigate. Cyberspace is, in fact, anti-spatial, because one cannot define where it is, nor describe its shape. In the analysis, particular relevance has been given to the geography of cyberspace, since thanks to the advent of cyberspace, geography has been reconfigured. In this sense, almost all Internet traffic is carried by undersea fibre-optic cables, and these undersea cables have been connecting countries since the 1980s. Therefore, cyberspace influences geopolitics and international relations, not only because the use of data by users is massive, and therefore, it is necessary to define security aspects related to data, but also because of the growing development of cyberspace in various sectors. Many global and regional organisations are involved in ensuring security and governance aspects in cyberspace. The need for this has proven to be so given the use of cyberspace by Islamic terrorism, in what is defined as cyber-terrorism. The term was first used in the 1980s by Barry Collin. Terrorists' use of computer and information systems has, over the years, resulted in strategic infrastructure attacks on government systems or networks, telecommunications, energy systems, water control systems, and other functions essential to society. Contemporary Islamic terrorism in particular is based on communication, and the use of cyber devices has represented an evolution also for terrorists, and it is not by chance that we speak of e-jihad. It was analysed how, in this sector, the use has been growing for several years, also given the presence within terrorist organisations such as al-Qaeda and ISIS of young people with skills and experience in the cyber sector. Finally, a space was dedicated to what is defined as 'independence in cyberspace'. Several examples of people claiming their own 'top-level domains (TLDs)' have followed one another, some of which have been declared as national symbols and 'flags in cyberspace'.

THE INSTRUMENT OF SANCTIONS

The next chapter was devoted to sanctions: sanctions are an instrument that has been used and conceived for many years within international organisations, and the analysis focused on the United Nations system and the European Union system. As

far as the Washington-based international organisation is concerned, a historical excursus on the use of the power of veto, which, especially in the early years of its activity, prevented the implementation of sanctions within the Security Council and, more generally, intervention in various crisis theatres, was useful. The types of sanctions imposed by the United Nations have changed and evolved over time. This aspect is fundamental for the analysis of the entire final work. After listing a series of measures that have been mostly imposed by the United Nations (Asset freezes, Arms embargoes, Travel bans etc.) and describing their characteristics, two cases of sanctions regimes adopted by the Security Council during the Cold War were analysed. Reference is made to the Apartheid South Africa and the Southern Rhodesia's case. The use of the so-called "comprehensive sanctions" had the objective of weakening the state economy to the point of forcing the government to change its position on the object for which it had been sanctioned. However, there was a downside to all this: it affected the civilian population in a massive way. Today, most sanctions are 'targeted', with the aim of maximising the impact on the individuals responsible for the violation and, at the same time, reducing the consequences in the population. In addition to UN sanctions, EU sanctions have been analysed. The EU has acted, firstly, with the aim of implementing and making more effective the sanctions imposed by the UN. Secondly, sanctions have become an instrument of the common foreign policy. The EU has therefore also used the instrument outside the UN framework, mainly with the aim of promoting human rights and democracy. The decision-making process regarding EU sanctions has been deepened. As with UN sanctions, a space has been dedicated to analysing in detail successive and ongoing cases of sanctions. The first case study was that involving the European Union and Belarus. Relations between these two actors have always been fluctuating: each step towards cooperation was matched by an equal and opposite one that seemed to move away from the previous one. The Brussels-based organisation considers itself ready to support a peaceful transition to democracy with various instruments, including an economic support plan. On the other hand, the transition appears to be very slow and complicated, with several problems to manage and for which the sanctions do not seem to fully meet the objectives for which they are imposed. Still in relation to sanctions, we wanted to dedicate a specific space to "energy sanctions" and their geopolitical significance. Therefore, an analytical framework called "the Rules of Six" is proposed, composed of six tactical interventions used by nations as a security policy tool to intervene in the energy markets. In the context of energy sanctions and their geopolitical significance, the troubled relationship between the US and Iran was explored, the relationship, to date, remains unclear and uncertain, despite indirect meetings in Vienna regarding the JCPOA.

CRYPTOCURRENCIES: UNDERSTANDING THE PHENOMENON AND ITS EVOLUTION

An entire chapter was then devoted to cryptocurrencies, their origins, working principles and characteristics that are useful for understanding the phenomenon and its evolution. Cryptocurrencies can be defined as a digital or virtual currency which, therefore, does not exist in physical form and is not tangible. Cryptocurrency derives its name from two words, namely, cryptography and currency; a digital currency controlled by cryptography.

A cryptocurrency has no inherent value; however, its value comes from the people's belief in it. Regarding its birth, the first cryptocurrency, which is also the most famous to date, is Bitcoin. Bitcoin was created on 31 October 2008 by Satoshi Nakamoto (a person or group of people whose identity is still unknown). The cryptocurrency actually owes its birth to the lack of confidence in the international financial system after the 2008 crisis, hence one of the great characteristics of cryptocurrencies: the absence of a central authority or regulatory authority. But the key word used in analysing the phenomenon, apart from the cryptocurrency itself, is definitely the blockchain. Blockchain could be defined as a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. Our relationship with money is guaranteed by the trust that people place in third entities regarding the security and privacy of their assets. The fact remains that these third parties can be hacked or manipulated and that is where the blockchain comes in. The potential of the blockchain lies in the fact that every transaction can be verified at any time without compromising privacy, thanks to the anonymity feature. Therefore, the two main features of the blockchain were analysed and explored: anonymity and distributed consent. What we also tried to explore were the applications that can be executed through the blockchain, both in the financial and non-financial fields. Next, much space was devoted to the mechanism that leads to the verification of the transaction by users who voluntarily provide their means and tools to solve complicated mathematical calculations based on an algorithm in order to add a block to the chain and be remunerated for it. The process is called 'mining' and the users 'miners'. In reality, the process of cryptocurrency mining, which also serves, at least as far as Bitcoin is concerned, to bring new cryptocurrency into circulation, has a number of implications and consequences that have been explored further. The strong and rapid evolution of the cryptocurrency market was then analysed with the rise of Bitcoin and the creation of numerous other cryptocurrencies currently on the market.

THE GEOPOLITICS OF CRYPTOCURRENCIES

It then looked at how international organisations have approached the phenomenon of "crypto-regulation". Cryptocurrencies and blockchain technology have posed complicated questions and challenges to policy makers, given the absence of regulatory frameworks. The initial position, especially on the part of international financial organisations, was to reject the consideration of cryptocurrencies as a currency, but rather to consider it as a speculative bubble, exploiting as a shortcoming what, in the world of cryptocurrencies, is a characteristic: the absence of a central authority. Subsequently, as usage has evolved, several organisations have expressed their concern especially with regard to the illicit use of cryptocurrencies, with real-world impacts, most notably money laundering and terrorist financing, and have begun to discuss organic regulation, which, for many international organisations, seems a long way off. There has also been an evolution in the approach by governments of different countries around the world to the growth of cryptocurrencies. G7 governments, for example, have recognised the need

for international cooperation on how private digital currencies should be regulated. Approaches have been different for many other states and, in particular, it has been decided to explore what has been done by China, Venezuela and El Salvador. In the last part of the chapter dedicated to cryptocurrencies, an attempt was made to analyse the future of cryptocurrencies, without wanting to answer in a clear-cut manner and without going into deep economic considerations, describing both the opportunities and advantages, the risks and threats and, finally, what could be the possible improvements to the system to reduce or eliminate the obscure features and to bring more people to the use of this instrument. The conclusion is that, both in terms of limiting misuse and in order to bring more people closer to the use of this tool, the involvement of institutions at national and international level is necessary, as well as the formation of a basic culture of the phenomenon.

HOW CRYPTOCURRENCIES ARE USED TO ESCAPE FROM SANCTIONS

The last chapter represents the central point of the thesis and aims to describe a little-known and very topical violation: the evasion of sanctions through cryptocurrencies. It is the chapter that includes all the topics mentioned and discussed above, in order to provide a broad and comprehensive overview. To describe the phenomenon of sanctions evasion, it was essential to mention what is defined as a great weapon in the hands of the United States and the European Union in particular: SWIFT (Society for Worldwide Interbank Financial Telecommunication). The mere threat of exclusion from this system, which has evolved considerably over the years and now comprises more than 212 countries, is a major alarm for states, with serious consequences and repercussions at an economic level. However, with the aim of describing the phenomenon in its entirety, the crypto-regimes of the European Union and the United States have been studied in depth. With regard to the European Union, the international organisation has made numerous efforts and great strides in both defining cryptoassets and regulating uniform rules for cryptocurrencies through a framework called "Markets in Crypto-Assets Regulation (MiCA). The point on which the European Union has focused most is certainly money laundering. In fact, the sixth directive against money laundering has been in force for all Member States since last December. As far as the United States of America is concerned, a primary role is played by the Treasury Department's Office of Foreign Assets Control (OFAC). OFAC has been cracking down on penalty evasion through cryptocurrencies and money laundering since 2018. OFAC has significantly increased its presence in the sector in order to regulate it by emphasising compliance obligations; these remain the same whether transactions are denominated in virtual or fiat currency and has begun to include in its list of Specially Designated Nationals and Blocked Persons (SDNs) virtual currency addresses linked to sanctioned persons. Another body, besides OFAC, that deals with regulation in the US and is also part of the Treasury Department is FinCEN (Financial Crimes Enforcement Network). The latter has been providing recommendations since 2013. The focus on the sector was also made explicit by Secretary Yellen, she argued: "The misuse of cryptocurrencies and virtual assets is a growing problem, too. I see the promise of these new technologies, but I also see the reality: cryptocurrencies have been used to launder the profits of online drug traffickers; they've

been a tool to finance terrorism." After analysing and delving into the crypto-regimes of the United States and the European Union, the focus was on the actors: who evades sanctions through cryptocurrencies? How does this evasion take place? Why are they evaded? The answer to these questions also leads to considerations related to geopolitics, both because of where the evasion takes place and because state actors are also involved. With regard to the first question, it was possible to analyse the evasion of sanctions by the following states: North Korea, Russia, Iran, and Venezuela. By analysing these states, it has been also possible to answer how the evasion takes place and why it is done. Regarding North Korea, the country started practising cryptocurrency theft. Another state involved in the practice was, albeit not directly, Russia. In 2019, the US announced sanctions against Evrofinance Mosnarbank, a Russian bank involved with the Venezuelan Petro. Petro's early adopters allegedly transferred funds to an account owned by the Venezuelan government at the aforementioned bank. Iran has been analysed as well: the Middle Eastern state has in fact developed a platform, IranRescueBit, with the aim of making donations through different cryptocurrencies (Bitcoin, Ethereum, Litecoin) in an easier way and this has represented a threat to the sanctions imposed by the US under Trump. The different strategies and methods that were used to circumvent the sanctions were then explained: cryptocurrency theft; cryptocurrency mining, which allows capital to be generated outside the financial system; the creation, as seen, of a national cryptocurrency; bringing together several states in creating a common cryptocurrency, this idea has recently been associated with the BRICS and the possibility of creating BRICSCoin, with the aim of fighting the hegemony of the US dollar and, finally, the fifth strategy lies in encouraging the population to use the digital currency, which is what is happening, with due particularities and differences, in El Salvador.

In conclusion, we wanted to find out how to curb this offence and how national and international institutions have acted so far. What seems clear by now is the need for a broad regulation that reaches as many states as possible. Although, in fact, many bodies have focused on anti-money laundering and combating financing terrorism (AML/CFT), action on sanctions evasion is still limited. With regard to regulation, it has been made clear that, in my opinion, total incorporation or attempts to replicate the system are unsuccessful. Cryptocurrencies were born in response to a lack of confidence on the part of many people, and I don't think this would be a viable way forward, or one that would have the desired effects. In the same way that global regulation is necessary, the way in which it is regulated should be such as to allow the phenomenon to develop, while maintaining certain basic rules to combat the financing of terrorism, money laundering, the evasion of economic sanctions and other types of crime committed through the instrument of cryptocurrencies. States and international organisations stand to win a major challenge in regulating this phenomenon, because providing a comprehensive framework also brings benefits to regulators. The benefits have already been seen with blockchain, a more easily embeddable and transferable mechanism, which responds to and facilitates various

tasks performed daily by states and organisations, allowing the distance between the citizen and institutions in general to be reduced.