University of Malta

POLICY AND REGULATORY CHALLENGES TO DEPLOYING BLOCKCHAIN TECHNOLOGIES

HANANE BOUJEMI

Dissertation submitted in partial fulfilment of the requirements for the degree of Master of Arts in Contemporary Diplomacy (Internet Governance)

Supervised by: Dr. Jovan Kurbalija & Vladimir Radunović

Faculty of Arts, University of Malta & DiploFoundation

December 2017

Acknowledgements

Sincere thanks to Jovan Kurbalijia for the guidance, Vladimir Radunović for the constructive feedback and Arvin Kamberi for the lively discussions about and genuine interest to help me complete this research.

“Success is not final, failure is not fatal. It is the courage to continue that counts.”

Winston Churchill

Abstract

Blockchain technologies are heralded by some as one of the most promising innovations after the Internet. The concept's origins are linked to Bitcoin, a paperless cryptocurrency, and the first decentralized digital currency that works without a central bank or single administrator.

The concept is generating worldwide interest because it challenges the status quo of centralised structures, and effectively omits intermediaries in exchanging values. Scepticism regarding whether or not blockchain technologies can deliver on their promise to omit centralised authorities is looming, however, due to the lack of concrete products to validate its use beyond the financial sector. Most of the ideas are still in the proof of concept phase, and most investments in these same concepts are merely speculative and are not representative of the real potential blockchain technologies offer.

The hype surrounding blockchain can no longer be ignored as news breaks everyday about blockchain powered products mushrooming all over the world; hence, it is crucial to research its technical parameters, understand them, and aim to define the main challenges we could potentially face if it is widely adopted. The current discussion trends in technology circles suggests that blockchain technologies will be at the centre of innovative solutions to almost every dilemma humanity is facing. If that is the case, though, there is a need to identify the regulatory and policy implications of blockchain deployment due to its distributed and transnational nature.

This dissertation provides overviews of blockchain's history to understand its origins before moving on to investigate its core features and how it qualifies as a disruptive technology. A descriptive section on how blockchain technologies work follows to provide a description of its technical foundation and how it links to the theory of decentralised systems.

The analysis extends to address the legal and policy implications of blockchain applications. The objective is to depict the importance of introducing regulation that promotes innovation and transparency in decision-making. Examples of governmental approaches in various jurisdictions then clarifies how regulatory frameworks are adapted to provide creative solutions to regulatory issues specific to blockchain technologies but without forgetting to present the legal challenges pertaining to their deployment. Additionally, the analysis explores to what extent the design criteria of blockchain technologies are compatible with currently implemented regulation.

Finally, this dissertation highlights the issue of the governance structure of blockchain technologies, and how it can hinder the evolution of this technology in the absence of a baseline good governance model that is not solely grounded in the good intentions of coders. The focus is then shifted to analyse how to build consensus around blockchain-related challenges, the transparency of relevant decision-making processes, the balance of power in blockchain technologies as distributed structures, and how to maintain the interest of the minority in a majority-based consensus mechanism on which blockchain technologies thrive.

Table of Contents

Chapter I

Introduction

By the end of 2017, Bitcoin fever reached its peak as the price of each Bitcoin was worth up to $20,000 at one point.[1] This incident was enough of a sign for anyone who did not know what Bitcoin is to actively seek an explanation. A simple Google search generates millions of entries to read about the digital currency: it is paperless money, generated by a cryptographic code; it is immutable, can be transferred over peer-to-peer networks, and no intermediaries are needed. It essentially means the end of exorbitant transfer fees, banks, and anything that stands in-between currency and the people that use it. The tension further mounted as news headlines raced to cover this unexpected development, the sprint to buy Bitcoins intensified, and everyone suddenly became a financial analyst, suggesting that now – meaning five minutes ago – was the time to invest. Speculating the future of this barely known product outside the crypto community meant that some people sold everything they own to buy Bitcoins; the banks, regulators, and governments, meanwhile, are watching the news unfold, trying to make sense of it all.

Volatility of prices is never positive news. When a currency or any product increases in value suddenly and exponentially, it attracts a lot of attention and almost always makes news headlines since it provides the perfect combination to generate interest among individuals who are willing to take the risk; it is a bubble. The price of Bitcoin eventually dropped significantly as an outcome of the rallying combined with many governments that took a stand against it by completely banning the cryptocurrency. This does not mean that Bitcoin is now history, as there is more to it than just being a digital currency. The underlying technology used as a core protocol that runs Bitcoin has been the centre of attention because it allegedly addresses the vulnerabilities of centralised structures. Blockchain technology simply is an inherent set of principles based on which Bitcoin functions; it is a chain of blocks where data is stored and distributed, which is tamper resistant, and cannot be corrupted.

Blockchain deployments are now an obsession, where hundreds of ideas are sprouting everyday with a promise to offer a blockchain-based solution even if it is unneeded. Blockchain as a concept is perceived to be a sound solution worth exploring to understand how it can be applied

[1] See: https://cointelegraph.com/news/bitcoin-hits-20000-per-coin-capping-year-of-enormous-growth.

and scaled; the issue is until now, there is little evidence that it works, hence the need to examine its limitations and how it fits into the current technological landscape.

Blockchain technology supporters believe it will generate significant economic benefits and shape global business operations through the Internet in the future. It is seen as an innovative solution that will advance all aspects of exchange; the best analogy is to think of it as a global transport system of values that offers the option to do business with people without trusting them. Instead, trust is generated by mutual faith in the technology's underlying principles governing the exchange. It sounds like the missing puzzle that complements the role of the Internet in connecting the world; blockchain technology could indeed be one of the next best innovations after the Internet itself.

This dissertation attempts to bridge gaps in analysis about the legal and policy challenges to the development and deployment of blockchain technologies, and it demonstrates the main challenges to its governance structure. The existing research on the topic mainly focuses on the technological aspects and programmatic language requirements but fails to investigate the impact of this technology on current regulatory frameworks, where the two must co-exist, and vice versa.

This research will endeavor to demonstrate the importance of tackling the policy aspects of blockchain deployments in order to mitigate the potential clash between technology and regulation. The outcome of the analysis will help define a roadmap of the elements to look out for during the implementation of blockchain applications beyond the technical parameters. The intention is to identify guiding points to regulators and policy-makers about relevant governance issues to ensure the uptake of this technology is not hindered in the long-term.

This research is conducted with full awareness of the scarcity of academic references and resources about blockchains' governance structure outside of the technical scope – meaning discussions about blockchain governance is occurring, but only in developers' circles. In addition to the technical parameters, most of the existing literature focuses on definitions, criteria, and case use. Nevertheless, the design of this dissertation evolves organically to address logical questions on blockchain governance once establishing a clear understanding of what blockchain technologies are and what they can achieve.

Setting the scene in the first chapter of this dissertation involves defining the concept of blockchain and highlighting its historical background, followed by a thorough description of its core features. A descriptive section on how blockchain technologies work then provides an

overview of its parameters. The second chapter focuses on analysing the policy implications, existing regulatory approaches, and if blockchain design criteria responds to the currently applied regulatory frameworks. The chapter concludes by addressing the current legal challenges that can affect blockchains' development and deployment. The third chapter highlights the issues concerning blockchains' governance structure by drawing an illustration based on two widely known blockchain applications: Bitcoin and Ethereum. The analysis then covers how transparent the decision-making and consensus-building processes are in permissionless blockchains. Finally, the last chapter concludes by exploring how to manage soft power accumulation in distributed systems, and how to maintain the interest of the minority in the majority-based consensus mechanism currently used by blockchain technologies.

Objectives

This dissertation's objective is to define blockchain technologies as a concept, their design criteria, and the legal and policy implications to their deployment. It presents an overview of the current regulatory challenges and the potential friction with currently implemented legislation in jurisdictions where data sharing is regulated, as well as how it can affect the uptake of this technology if not addressed in a timely manner.

Finally, it will address the question of blockchain governance, highlighting how it is subject to scrutiny due to the current technical limitations and system vulnerabilities. Additionally, the research highlights the roles of all stakeholders vis-à-vis the current governance structures of currently operational applications such as Bitcoin and Ethereum, and what those models mean for transparency in decision-making processes within these blockchains.

Research Methodology

This dissertation presents what blockchain technologies are and identifies the core features that underpin their ability to be an innovative and disruptive technology. Historical background is provided to identify the origins of blockchain technologies and how they work. The hype about blockchain technologies drives more attention to their economic benefits, whereas there is a significant vacuum in analysing the potential policy and legal challenges blockchains will trigger when and if they are deployed at large scale.

The available research on blockchain technologies largely focuses on their technical aspects; although this is undoubtedly important, there is an urgent need to explore the policy implications for blockchain technologies since it is indispensable to technological advancement. The research methodology of this dissertation focuses on providing a comprehensive policy analysis basing on existing literature about the topic. Specific attention was given to drafting a detailed outline based on which the corresponding literature is defined. Explaining the concept, for example, required cross checking different sources before summarising the main reflections points. It was important to identify literature which tackle the subject from diverse angles: technical, practical and use case. Equally crucial was to read research supportive and opposing to the technology since there is . The outline was revised numerous times following guidance from the supervisors who provided a list of readings relevant to each chapter to help build arguments about the chosen topics.

The main goal of this research is to uncover and analyse the potential regulatory and policy issues surrounding blockchain technologies, but not necessarily provide a solution to them. The goal here is about demonstrating how regulation or the lack thereof contributes to the sluggish uptake of innovations such as blockchain technologies. Therefore, the literature identified to find this specific type of information was diverse and included reports, articles and op-eds and not only books. While the current trend of analysis mainly focuses on the technical aspects of blockchain products, this research raises policy-based questions on the concept of trust, why blockchains qualify to replace centralised systems, blockchain governance structures, and how to manage soft power accumulation within a distributed setting. Therefore, extrapolation was utilised to present the concepts in various occasions. This research explores the link between the notion of trust, innovation, and regulation with an emphasis on highlighting the two interacts in various contexts. This triangle is at the core of blockchain deployment as it triggers legal and jurisdiction questions due to the decentralised nature of applications. This specific

point required thorough research to define the various existing point of views by the developers' community usually published in a personal blog.

It was challenging to find publications to address blockchain governance issues. However, designing an outline specific to existing practices was crucial to jump start an objective analysis on blockchain governance so part of the information was gathered from the bibliography used in other chapters. It was important to define publications which addressed the governance question with sharp focus on their core design criteria of open access, inclusiveness, and distribution of control among the networks where they operate. The intention is to gauge the criticism of blockchain technologies, specifically public ones, are subject to due to their current governance setting, which is based on consensus building in managing the code – a rather unconventional form of governance that only appeals to technologists and the enthusiasts about blockchain, but not traditional structures where decision-making is centralised and good governance mechanisms have formal, pre-set criteria. This research showcases two existing governance models of widely known blockchain-based cryptocurrencies, Bitcoin and Ethereum, and depicts to what extent their governance models can or cannot be applied in order to judge if these concepts are qualified to act as a legitimate substitute to centralised forms of power.

Finally, the analysis elaborates at a basic level on how soft power accumulation in distributed structures is manifested within blockchain technologies. How it could potentially affect the balance of decisions, and how to safeguard minority interests in majority-based consensus systems.

Literature Review

The literature review consists of all the key publications by authors concerning the subject area and their findings. Even though the scope of the research is specific, and the policy discussions are still in their infant stages, it was very helpful to read a number of publications that become key to this dissertation. Defining concepts is crucial to understand the ethos of blockchain technologies. The field is fueled by technical terms, which can be complex to understand in the context of contemporary diplomacy. In fact, it might appear that both disciplines are quite distinct; based on my experience with various Internet governance processes, however, grasping technological concepts is critical to identify the nexus between policy and technology.

Then comes the role of diplomatic skills and knowledge, which were thoroughly covered in the study modules of this master's degree, to negotiate or discuss the issues at stake at government level.

One of the key publications that helped increase my knowledge about the subject area and identified a key gap to explore further was *Mastering Blockchain (*Bashir, 2017). The book provides a fundamental overview of blockchain technologies, ensuring that the basics of the topic are clear before gradually explaining the theoretical and technical principles underpinning them. The more his descriptions dive into details, the more complex the narrative becomes. It was important to define the technical concepts in a simple fashion before embarking into a more in-depth analysis, and this book was very helpful in outlining those fundamentals. Note, however, that the book requires some knowledge about technical concepts such as cryptography, – an important component in the functioning of blockchains, which needs to be addressed in a comprehensive manner. The clear descriptions throughout the book of such concepts made it easier, though, even though the applicability of the concepts listed could be stronger in order for the reader to have a clearer understanding of how blockchain technologies apply to everyday life.

A key publication that does exactly that is by the Tapscott brothers *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World* (Tapscott and Tapscott, 2016). It is practically the first book to explain why blockchain technologies could fundamentally change our lives. The authors went to a great length to illustrate how blockchain applications can effectively solve current dilemmas around transparency and decentralisation of decision-making. The authors provide ample examples to demonstrate how blockchain technologies will shape the future of the world economy as well as many aspects of day-to-day life. The book is well researched and highly accessible, but some chapters include summarised interviews, which could be synthesised better to capture the main points of the subject matter. The same authors have also published an important report for the World Economic Forum (WEF) which was in the dissertation *Realising the potential of Blockchain: A Multistakeholder Approach to the Stewardship of Blockchain* the report presents an important opinion about how blockchain will constitute a generational shift from the Internet of information to a new-generation Internet of value. The authors stressed the importance of forming a multi-stakeholder consensus mechanism around how blockchain technologies function from the technical, regulatory, and economic angles to create an enabling environment for them to succeed.

The dissertation includes a wide range of articles and research papers that specifically discuss the various aspects of this dissertation. It was important to derive information about current developments from the source. For example, discussing blockchain policy challenges, especially privacy, required consulting articles by Vitalik Buterin who extensively explained the concept in "Privacy on the Blockchain" (Buterin, 2016). His work was also instrumental to drawing a clear line between decentralisation and distribution; these two concepts are often confused with each other, but his article on "The Meaning of Decentralisation" (Buterin, 2017) helped define the difference between the two concepts.

The literature on defining and analysing the regulatory and policy challenges to blockchain technology deployment was derived from publications highlighting the legal limitations, such as Norton Rose Fulbright's (2016) '*Unlocking the Blockchain: A Global Legal and Regulatory Guide*. It was very useful to derive the major legal challenges according to practitioners at the forefront of negotiating traditional contracts, which will be presumably replaced by permissionless systems powered by blockchain technologies. The policy scope was derived from the core functions of blockchain technologies, and mainly focused on their privacy and security. In this regard, "Hidden in Plain Sight: Transacting Privately on a Blockchain" (Olg, 2017) identifies a practical solution to blockchain privacy issues.

It is important to note that literature on blockchain governance is scarce since it is a relatively new technology. Regardless, the bibliography includes some of the early analyses of the concept, such as "Governance in Blockchain Part I: The Bitcoin Experiment" by Wang (2017). It delineates the parameters of governance mechanisms that should extend to include a wider range of issues than merely focusing on blockchains protocol governance, in other words how the code of blockchain applications is governed.

Chapter II

1. What is Blockchain? Definition & History

Blockchain technology allegedly revolutionises transfers and exchange procedures over the Internet across various sectors. It is designed with an inherent capability to trust the contracted parties without the need of an intermediary because it relies on a distributed, encrypted, and irreversible system of authentication. This means once a transfer of a contract, money, or data is recorded on the chain, it is unlikely possible to reverse or change it. These criteria are perceived to be crucial to deliver transparent and accountable business operations or government services without the need of an intermediary. Blockchain enthusiasts believe these properties will radically change the economic landscape and accessibility to global markets by creating a new business model that places the end consumer as the primary beneficiary. Vitalik Buterin, the founder of Ethereum – the second largest blockchain after Bitcoin – thinks that while "most technologies tend to automate workers on the periphery doing menial tasks, blockchains automate away the centre. Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly." Blockchain sceptics, however, fear that the hype around blockchain technologies has reached the trough of disillusionment and will unlikely deliver on its promise as the next best thing.[2]

It is the early stages of blockchain's adoption, and there are various interpretations to what the technology means for society, and what it can and cannot deliver. The first chapter of this dissertation defines the concept and principles of blockchain technologies according to the existing literature, and provides an overview on its genesis, history, features, and design principles to present clear understanding about its potential.

[2] Trough of disillusionment is a term used by Gartner Hype Cycle to describe when interest in a technology wanes as experiments and implementations fail to deliver, and producers of the technology shake out or fail. Investments continue only if the surviving providers improve their products to the satisfaction of early adopters. See more at: https://www.gartner.com/technology/research/methodologies/hype-cycle.jsp.

1.1 Blockchain Definition

Blockchain is a digital, decentralised public record known as a ledger[3] of continuously growing transactions listed in chronological order that are linked via cryptography.[4] There is no consensus over a specific definition of blockchain as a concept, but most of the authors of the references consulted provide a provisional definition, which includes a literal description of blockchain's features using identical key terminology. Some authors even stated that the term is ambiguous and has different meaning for different people depending on the context (Drescher, 2017). This is partially true because blockchain has been widely conflated with Bitcoin, a cryptocurrency invented and launched in 2009 by the pseudonym Satoshi Nakamoto (Hofmann et al., 2017). Bitcoin actually integrates blockchain as a core technology to exchange transactions securely and anonymously (Maelo, 2017). Its launch generated mixed views ranging from hyped enthusiasm from avid technologists, to sceptics critiquing the viability or even the need of having a digital currency. In fact, Bitcoin discussions took over the global tech scene to the extent that it completely obscured the technology behind it, blockchain. More elaboration on this specific point will be covered in the following paragraph on the history of Blockchain, for now I will focus more on the definition.

The confusion over the definition of blockchain stems from the complexity of the technology itself, even though the idea behind it relatively simple and straightforward: provide the ability to exchange transactions anonymously and securely without an intermediary (Tapscott and Tapscott, 2016). As such, blockchain incorporates a core function that can be defined from two angles: the business side and the technical side. From the business perspective, blockchain is a platform whereby peers can exchange values without the need of approval from an intermediary or central authority (Bashir, 2017). This model of exchange entirely relies on the users of the blockchain database being publicly accessible to the participating nodes (a computer connected to the network). Each connected node receives a copy of the blockchain, which has records, and stands as proof of every transaction ever executed (CFA, 2014). This empowers the blockchain as a decentralised consensus mechanism where no single authority is in charge of the database (Bashir, 2017). Evidently, the concept reinforces the principle of trust among the contracted parties traditionally guaranteed by a central authority, which is

[3] A ledger in accounting is a book that classifies financial information, including debit/credit transactions, and shows current balances. See: http://www.businessdictionary.com/definition/ledger.html.

[4] Cryptography is the science of transforming information into a secure format via encryption. See: https://techterms.com/definition/cryptography.

essential in any business operation. Grasping the business angle of blockchain does not seem to be sufficient to scale it, however, because its deployment requires clear understanding of (1) the specific technical properties, and (2) if they meet the real-world application requirement to deliver a viable business model. This might explain why the adoption of blockchain has been sluggish in fields other than the financial sector.

From the technical perspective, a blockchain can be trusted as an exchange channel because it offers the possibility to permanently process and store encrypted transactions. It also records all transactions, making it impossible for a user to modify the ledger once a block in a blockchain has been sorted. Blockchain technologies provide a way to securely and efficiently create a tamper-proof log of sensitive activity since each set of transactions are stored in a block linked to the preceding one (Meola, 2017). This creates an immutable chain of transactions that is permanently time stamped. It is therefore impossible to alter the contents of any transaction without taking control of most nodes in the network and rewriting the parameters of all subsequent transactions in the chain.

According to Bashir (2017) there are various technical definitions that could be summarised as follow:

- Blockchain is a decentralised consensus mechanism where all peers come to an agreement regarding the state a transaction.
- Blockchain is a shared distributed ledger of transactions and a single source of truth for all member organisations using it.
- Blockchain is a data structure using hash pointers linking to the previous blocks.[5]

Based on the above definition, the major innovation of blockchain from the technical point of view is the ability to build trust in a transaction based on a unanimous, algorithmic consensus mechanism. Such mechanism allows market participants to approve and transfer assets across the network, which subsequently authorises the generation a new block in the chain. A block is the most "current" part of a blockchain, which records all the transactions in proper linear and chronological order (Meola, 2017). Every block contains a hash of the previous block,

[5] A hash function is a function, mathematical or otherwise, that converts a numerical value into another fixed numerical value. The value produced includes the unique set of bits called a hash that can be sent with a message. The point is to fingerprint the message for the receiver to verify its authenticity by comparing the hash function replicated with the one received, as they must be identical. See: Schneier (1996).

which makes each one of them unique and irreversible. For instance, Bitcoin uses a Proof of Work (PoW) algorithm as a consensus mechanism to validate the generation of blocks.[6] It is the most commonly used consensus mechanism employed by blockchain technologies, and it is meant to be the seal of approval to the state of the ledger. In sum, both the business and technical definitions of blockchain focus on the feature of decentralisation, distributed decisions powered by machine-driven consensus mechanisms, anonymity of the exchange, and irreversibility of transactions that lead to instilling the principle of trust. These definitions, however, fail to provide a comprehensive explanation of the underlying technology behind blockchain; what sort of formula or algorithm is used to generate an automatic order of the blocks in the chain, for instance? Moreover, it does not address who or what is behind the technology, and to what extent it can be trusted as an instrument that shifts power from away from existing intermediaries?

The next paragraph will provide an overview on the genesis of blockchain technology, shedding the light on its background and its origin – a difficult task given that the inventor(s) is/are still anonymous.

1.2 The History of Blockchain

Blockchain's history is relatively short, recent, and tightly linked to Bitcoin. As stated earlier, blockchain is the inherent technology used to operate Bitcoin, a cryptocurrency that was launched in 2009 by a mystery inventor or entity named Satoshi Nakmoto, and there is no confirmed information if this name can be attributed to a person or a group of inventors. According to the white paper introducing Bitcoin as a peer to peer electronic payment system[7] , however, the name traces back to a Japanese-American living in Southern California, who persistently denies, until today, that he is the person behind inventing Bitcoin.

Uncovering the identity of Bitcoin's inventor has been a prime concern of the cryptocurrency community and several media outlets. It was defined by *The New Yorker* as "one of the most compelling stories in technology" (Chen, 2016). While everyone is curious about the identity of Bitcoin's inventor, the decision to remain anonymous may be deliberate. It may well validate

[6] A proof of work is a piece of data that is difficult (costly, time-consuming) to produce but easy verifiable by the network. Proof of work must fulfil certain requirements, and it involves many trials and error before a valid one is generated. For more information, see: https://en.bitcoin.it/wiki/Proof_of_work.

[7] The white paper outlining Bitcoin protocol was first published in 2009 and is available on bitcoin official website. See: https://bitcoin.org/bitcoin.pdf

the concept of trust based on which blockchain technologies operate, promising that one does not have to verify, in real life, the identity of the contracted party to trade. The increase of Bitcoin adoption in business operations demonstrates the technology behind it is trustworthy since decentralisation as a concept appeals to the public. Therefore, it is safe to assume that the mysterious identity of Bitcoin's inventor(s) did not affect its popularity or value. It certainly did trigger a wave of theories among the sceptics, though. For instance, unverified reports claim that the National Security Agency of the United States (NSA) managed to identify Bitcoin's inventor using stylometry[8] to develop a writing style for Satoshi in order to trace him, following concerns that he is a Russian or Chinese agent trying to undermine the U.S. economy (Haring, 2017). These claims have been neither not confirmed nor refuted by the NSA, so the issue continues to generate a fair amount of controversy.

The importance of identifying Bitcoin's inventor could demystify the chain of ideas tangled in a web of assumptions about the motives behind launching it. It could help us uncover the history of blockchain, as it as well as the inventor are both indispensable to each other. In fact, it is impossible to explain blockchain without referring to Bitcoin because it is a concrete example of how blockchain technologies are supposed to work (Adams, 2016). Satoshi's invention builds on technological concepts previously proposed by other researchers and technologist. The Proof of Work mechanism, for instance, was originally proposed by Cynthia Dwork and Moni Naor to fight spam in their 1992 paper "Pricing via Processing or Combatting Junk Mail."[9] In 1997, Adam Back drafted a similar proposal and called it Hashcash,[10] which would eventually underpin the PoW mechanism currently used by Bitcoin. It might be a futile exercise to trace back the motives of inventing Bitcoin because necessity invokes innovation. One particular analysis stressed that blockchain could have solved one of the issues partially responsible for the 2008 global financial crisis. Due to how the lending process worked at the time, settling lending transactions took many days. This meant banks and other financial institutions struggled to say exactly who owned what, and as a result, it was hard to judge their exact credit-worthiness. Without knowing that, these institutions were reluctant to lend (Williams-Grut, 2016). In essence, the timing of Bitcoin's launch in 2009 could be linked to the crisis because it serves as a logical response to what went wrong: the collapse of major regulated financial institutions was resolved by a bailout from the U.S. government using

[8] The statistical analysis of variations in literary style between one writer or genre and another. See: https://en.oxforddictionaries.com/definition/stylometry.
[9] The original webpage that discusses the concept is available at: http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp_abs.html.
[10] The email exchange where Adam Black first listed the script of a Hashcash and requested feedback is available at: http://www.hashcash.org/papers/announce.txt.

taxpayer money, which did not only affect the world financial order, but it also triggered major trust concerns by citizens in a centralised system.

The history of blockchain might be short and recent, but the potential impact of the concept is immense. Beyond cyrptocurrency and finance, the technology is now being tested for a number of proposes and industries, including combating human and sex trafficking, travel bookings, land registration, and electronic voting (e-voting). Technology entrepreneurs and business analysts vouch for blockchain as the next biggest innovation after the Internet itself because it addresses the issue of trust and removes the uncertainty implied by the virtual network(s). It is important to highlight that while the full capabilities of blockchain have not yet been fully unveiled, specific features define the technologies themselves, which the next section of this chapter elaborates upon.

2. Overview of Blockchain core features as a disruptive technology

Blockchain at its core is a peer-to-peer distributed ledger that is cryptographically secure, immutable, immune to tampering, and updateable only via consensus agreement among the network peers. In essence, the technology is designed to protect against domination of the network by any single computer or a group of computers (Richards, 2016), which presumably means the assets stored in the Blockchain network are safer than traditional storage mechanism because of the decentralised nature of the technology. The owner has direct access to the asset via a private key, a secret number used to generate a signature for each blockchain transaction and can transfer it whenever desired and to anyone without the obligation to run it through an intermediary.

Moving around assets on a blockchain is fairly easy for people who have a technical background. Doing so may pose a challenge for an average person to grasp the basics of sending and receiving transactions, however. The easiest way to understand the process is to think about how an old-fashioned mailbox system functions. As an example, X wants to send mail to Y. First X will need to know the mailbox address or number of Y. The same applies when sending Bitcoin. X needs to know the Bitcoin address of Y, a number that is uniquely attributed to him/her, and is also called a wallet address, or public key. Once the Bitcoin is

received, Y can view it in his/her wallet (mailbox), but to send it to someone else, Y needs to use the private key of the intended receiver, Z.

Blockchain is a disruptive technology because it supersedes the need for a central authority entrusted with the role of authenticating third parties to perform an exchange. Instead of placing ones' trust in a single entity like a bank or a government, the network of computers, where the proof of assets is stored, provides the permission to transact. The seal of approval embodies all the core features of blockchain technology, which includes six primary features: Distributed consensus, peers value transfers, transaction verification, security, immutability and uniqueness, and smart contracts.

1. *Distributed Consensus*

This is the principle underpinning a blockchain that enables it to present a single version of truth that is agreed upon by all parties (Bashir, 2017). It consists of the standards and rules for how every node exchanges the particular blockchain technology's information, the mathematical rules for all nodes to agree on to verify the integrity of that data, and the payment incentive(s) to support the consensus model. A key point of the entire platform is a method to ensure all transactions are validated once where no valid transactions can be omitted (DTCC, 2017). This key feature fulfils the role played by a central authority in the current markets, which is hieratically higher, and bound by manmade regulatory frameworks susceptible to change or that can be adapted to market conditions. This bring us to another functionality of blockchain technologies, which omits the hierarchy in decision-making relating to the verification of an exchange on the chain, and what is commonly known as peer-to-peer value exchanges.

2. *Peers Value Transfers*

This feature allows the assets to be produced and managed entirely within a specific network. It enables the transfer of value between its users via tokens, which bare the value of the product (Bashir, 2017). For example, Bitcoin's blockchain exists in a pre-defined grid where both the history and the quantity of every movement is mathematically verifiable in the distributed ledger of the network (DTCC, 2017), and it is available in chronological order. A blockchain

pushes for decentralisation via peer processing at its node locations. Transactions are verified at the peer-to-peer level no matter where the node is located in that network (Mougayar, 2016), as opposed to centralised systems where it is mandatory to have a vetting mechanism to validate transactions. The decentralised nature of blockchain technologies gives equal opportunity to all the participating nodes in the network to offer services based on their knowledge of the transaction taking place in the network they are part of. For the sake of conceptual clarity, Figure 1 below provides a comparison between the two models to showcase how peers are illustrated in a decentralised structure.

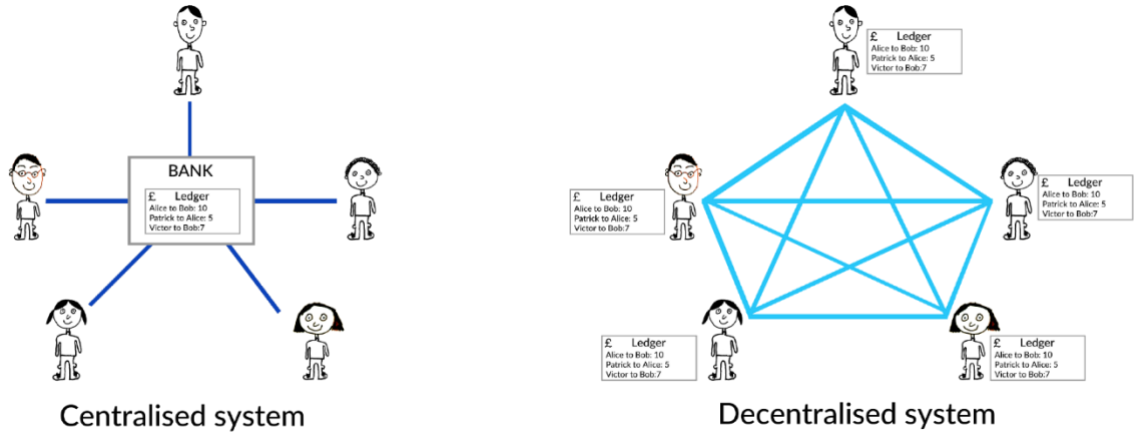

Figure 1 – source: https://medium.com/swlh/explaining-blockchain-with-wheres-wally-and-a-camera-79e860a05815

3. *Transaction verification*

Every transaction record is linked to previous transactions and is standardized for every participating node. Therefore, it can be easily traced in the network (Bashir, 2017). Every ledger entry is broadcasted in the entire network where all peers can verify its correctness, and is retraceable across its full history so it can be reconstructed. There is a standard network protocol that allows every participating node to receive every transaction publicly and apply the same validation rules including verifying: the signature, format, and the correctness of the fields (Karame and Androulaki, 2016). This protocol was mainly used to verify Bitcoin transactions to avoid double spending of a coin in a network. The verification process is done instantly or transcribed into a record and placed in a queue; in this case, the nodes determine if the transaction is valid based on the set of rules the network agreed on.

4. Security

Information data security management relies on a widely applicable model based on confidentiality, integrity, and availability of data known as CIA triad. These three elements are essential to protect unauthorised access to the data, to prevent any unauthorised change, and to ensure availability to access it when needed (Andress, 2014). These are the basic principles of cryptography, a mathematical theory converting plain text into unintelligible text and vice versa and transmitting it in a specific form that is only accessible to the intended recipient. In order to ensure the integrity and availability of data, blockchain uses cryptography where individual parties are never identified to the network. Instead, security keys are required to gain access to the transaction. All data entered into the chain is encrypted, and every user on the network is assigned their own private key. Though the blockchain is publicly available, it is protected with end-to-end encryption. For instance, when X deposits Bitcoin in Y's wallet, anyone in the network – including X – can peek inside the wallet and see the Bitcoin without having to share their identity. No one, except for X and Y, will know it belongs to Y, however.

5. Immutability & Uniqueness

The records are unique and immutable once added onto a blockchain, which means they cannot be altered or changed. If any changes are made on the public blockchain, everyone can view them. It is possible to roll back the changes if approval is granted by all the previous blocks that have already been added to the blockchain. This is considered impossible to do, however, because it requires a massive amount of computing power and bandwidth.

6. Smart Contracts

Blockchain provides a platform to run smart contracts that enforce the contractual rights of multiple parties. These are autonomous programmes that reside on the blockchain and encapsulate business logic and code in order to execute a required function when certain conditions are met (Bashir, 2017). This feature allows the digital codification of legal obligations, which provides a means of assigning usage rights to another party (Tapscott and Tapscott, 2016). It also allows owners of assets to code their requirements into contracts to clearly enforce their rights. For example, the music industry could benefit from this by ensuring

the copyright holders (artists, producers, promoters, etc.) are paid out automatically when their material is used. Specific conditions that outline the rights and obligations of all parties will form the business logic that these smart contracts provided for that the material stored on a blockchain . This could eventually end large-scale piracy in the digital age and facilitate fair pay of rights holders.

Blockchain incorporates features that enforce a set of rules to transfer assets on a network, has built-in security, and maintains internal integrity of its own history. In theory, if blockchain technologies function as they are designed to perform, it will challenge the concept of centralized power that is usually held by a handful of individuals or institutions. There is certainly space for this technology to thrive because the systems in place, political, financial, or others with existing rules, have proven to be non-representative and susceptible to manipulation.

It is very difficult to assert that good governance will be achieved if we move from centralised to distributed power. Just because it is more efficient to focus on building a technology that delivers service-oriented products rather than aiming at changing a system does not translate to an instantaneous revolution. Change is usually a long process that tends to face resistance, while technology is evolving faster than regulation and policy can keep up. If technological developments appeal to the needs of the system, their adoption would mean an improvement in service delivery but without necessarily challenging its authority.

Despite the excitement around the concept, it is important to note that some of the features blockchain technologies thrive on have been challenged in practice. For example, the fact that all Bitcoin transactions are visible to anyone in the network reinforces the principle of transparency; however, it also means that privacy is not provided. This has been the main barrier for its adoption by financial institutions and other industries that require privacy and confidentiality of transactions (Bashir, 2017). Nevertheless, developers are working on defining suitable solutions that guarantee the confidentiality of assets but still allow for the validity of transactions to be verified.

One developer, Oleg Andreev,[11] presented a new concept in 2017 called Confidential Assets, which asserts the scheme “enables both confidential and non-confidential assets to co-exist on

[11] Software designer and blockchain protocol architect.

a single blockchain and allows for selective disclosure of private data to designated third parties. It makes privacy a native feature of [blockchain technologies'] data model and architecture, not an add-on or special out-of-band case. It is compatible with blockchain programs, and relies on established cryptographic primitives that allow us to optimize for performance and scalability" (Andreev, 2017). If this concept is put into practice and proven workable, it could solve blockchain's privacy concerns. Otherwise, there are no concrete examples yet demonstrating that privacy can be guaranteed on a blockchain.

The security and immutability features of blockchain were put to test following two major hacks in 2016[12] and 2017.[13] Both incidents involved diverting Ether[14] cryptocurrency (Ethereum)[15] to false accounts due to a security vulnerability.[16] The 2016 incident was resolved by reversing the transaction, forcing the return of the funds to a replacement "recovery contract" validated informally on the network. This decision generated a considerable amount of criticism within the Ethereum community because it damages the blockchain's reputation for being unchangeable. This implores the question if a code-generating algorithm could address such vulnerabilities, or if human interference is mandatory in order to instil trust back in the network. Ethereum places significant faith in the code to generate smart contracts, which are less susceptible to manipulation. In this specific case, a decision had to be made that only a human could make. It occurs that reversing the transactions to address the hacks might be contradictory to blockchain's promised immutability feature. Yet, it also shows how the transparency and communal nature of blockchain transactions at this stage might be more important than the now-questionable claims that blockchains are immutable (Parker, 2016). The main concern is to safeguard the integrity of the network to maintain its value, which also means blindly trusting a leader, such as Buterin, the lead developer of Ethereum, to champion any radical changes of this sort. It is similar to the faith placed in political leaders to instil people's trust in a system.

It is important to note that the 2017 hacking incident was slightly different since it was triggered by a vulnerability in the stolen wallets, which meant that the transactions could not be reversed.

[12] Millions of dollars were diverted from Ethereum to a false account. See: http://techportfolio.net/2016/07/blockchain-hack-reversed-while-banks-look-on/.
[13] Another incident took place where a hacker stole 31 million worth of Ether by exploiting a vulnerability in the system. See: https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce.
[14] A cryptocurrency used to incentivise developers to write good applications on the Ethereum blockchain. See: https://www.ethereum.org/ether.
[15] Ethereum is an open-source, decentralised software platform launched in 2015, and is the second-largest blockchain after Bitcoin.
[16] See: https://www.coindesk.com/understanding-dao-hack-journalists/.

The solution decided upon by the Ethereum community included exploiting the same vulnerability the hacker used to stop the robbery (Qureshi, 2017). Such incidents certainly challenge core features of blockchain technologies, but they are also a catalyst to better understand its vulnerabilities given that blockchain adoption is still in the experimental stage in various sectors. As a concept, blockchain is certainly an innovative solution to move trust judgment to the code in areas where humans have failed to be fair. Yet, the technology is still limited, and must be put to practice to fully understand how trust mechanisms can be implemented without human interference – and if that is even feasible.

Looking at every single property of a blockchain in isolation might not seem remarkable. When combined, however, new properties appear that in turn create the possibility for new revolutionary use cases. It might be complex to explain how blockchain works to an average person, which means its audience is limited. Nevertheless, it is generating enough interest among coders, early investors, progressive governments, and corporations because, historically, the front-runners in the technology field are the ones who can spot the potential of new concepts early on and invest in them financially or by using their know-how.

Focusing on identifying and explaining the features of blockchain technology is vital to building common understanding of its benefits. This section specified the core characteristics of blockchain to pin down the reason why it is considered a disruptive technology, and the biggest breakthrough of the modern age after the Internet. The answer is because it provides a cutting-edge solution to trust issues on virtual networks, a major vulnerability of the Internet, and because it challenges the status quo of centralised power. As Buterin (2017) underscored, "The blockchain has the ability to enhance reliability in business processes by eliminating political and economic risks associated with trusting a centralized system." These motives are justified because of the inefficiency of centralised structures where resources are misused, and large segments of the society are marginalised because the entire system is serving a handful of people. There is a trust crisis in the system, and it is not clear yet if blockchain is the magic bullet to solve this dilemma. The next section will specifically elaborate more on how blockchain qualifies as a trust mechanism.

3. The concept of trust in blockchain deployment

Blockchain uses Decentralised Ledger Technology (DTL) that keeps a record of all transactions taking place across a peer-to-peer network. This means a blockchain has complete information about different user addresses and their status right from the genesis block to the most recently completed one. The blocks are added through cryptography, ensuring that they remain meddle-proof; the data can be distributed among peers, but not copied. Even though the ever-growing size of blockchains is considered by some to be a problem, creating issues of storage and synchronization (Meola, 2017), the rationale behind the process integrity qualifies the assets on a blockchain to be trustworthy among the participating nodes.

In general terms, decentralisation in technology "takes over the control from the government and central entities to the peer-to-peer network with immutable mathematical logic that provides better security, efficiency, and resilience with reduced timeframe and overheads" (Asharaf and Adarsh, 2017). The idea behind decentralisation in blockchain aspires to establish a system of checks and balance in consensus building as well as to democratise decision-making. In theory, this means the more decentralised consensus is scaled, there are fewer chances that the outcome decisions are untrustworthy. Therefore, decentralisation motivates trust on a blockchain by design because no single authority is in control.

The idea of omitting an intermediary through decentralisation in decision-making is appealing; however, the concept is currently generating heated debate among the blockchain community because of recurrent misinterpretations of what it means in Staoshi's 2009 white paper on Bitcoin (Jia, 2016). The feature of decentralisation is the raison d'être of blockchain technologies, but it seems that industry speculators and sceptics dispute its merits. It appears to be quite easy to discredit its viability since the concept is subject to different interpretation, and due to the lack of understanding of how it functions beyond Bitcoin.

Surprisingly, it takes a blockchain programmer (not to be confused with a web programmer) to explain how the code would achieve a truly decentralised ecosystem; one explanation by Jia Chang concludes that decentralisation on the blockchain is measured by "the degree of freedom allowed for joining in the consensus-making. Given that the codes are open source and that this information is equally accessible, freedom of decision-making is an indication of fairness where one enjoys the power to participate, as well as the power to quit." (Jia, 2016). In other words, the flexibility provided by decentralised structures on the blockchain democratises the

spectrum. This allows contributions in the decision-making process on equal footing, hence it strengthens the principle of trust in the code.

Another point worth highlighting is how the decentralisation of decision-making on the blockchain is often confused with distributed consensus – even though the two concepts are distinctive. Buterin provided a logical explanation for why both concepts are linked but simultaneously independent of each other. The basics of the matter boil down to understanding the difference between architectural decentralisation (how many computers is a system made of), political decentralisation – who are the individuals or organisations controlling the foresaid computers – logical decentralisation, and whether or not the system can operate independently if divided (Buterin, 2017). This leaves a pertinent point of reflection on the odds a blockchain could be dominated by one single authority, organisation, or group without detection. The author asserted that blockchains "are politically decentralized (no one controls them) and architecturally decentralized (no infrastructural central point of failure), but they are logically centralized (there is one commonly agreed state and the system behaves like a single computer)"(Buterin, 2017).

Decentralized blockchain technologies intend to balance out centralized authority with their strong consensus, privacy protecting focus, which will provide a powerful set of checks and balances on the excesses of centralized systems. It occurs in this specific circumstance that the buy-in to the technology behind the concept is much more important than trust because the latter is inherently guaranteed by design in a blockchain.

The familiarisation with blockchain technologies core features helps form an opinion about its potential. Nevertheless, it is crucial to understand how this technology works to outline how it can serve its purpose at the macro level. The next section will define how blockchain works by covering its generic elements and technical aspects at the operational operating level.

4. Blockchain non-technically: how does it work?

Blockchain technologies are have the potential to impact every aspect of our lives. The current trend of their deployments suggests that it can be applied to various sectors, including finance, healthcare, government, insurance, humanitarian work, and the entertainment industry. Blockchains are a novel approach to the distributed database because they incorporate old technology in new ways (Laurence, 2017). Traditionally, databases and application servers are under the control of a central authority, such as a system administrator or online service providers, namely Google, Amazon, or Alibaba. This model has changed now that blockchain technology allows anyone to start and operate a decentralised system with no single point of failure or a single trusted authority (Bashir, 2017). While it is important to identify the technically generic features of blockchain technologies, the conceptual understanding of their technical foundations is necessary to grasp how a blockchain-powered application operates.

The technical foundation of blockchain is tightly linked to the theory of decentralised distributed systems, which can be defined as a "computing paradigm whereby two or more computers (nodes) work in a coordinated fashion to achieve one common outcome" (Bashir, 2017). All the nodes are considered as an individual player in a distributed system, and all of them are capable of sending and receiving messages among each other in a peer-to-peer fashion. The advantages of distributed systems reside in the fact that they generate higher computing power as a result of the interconnection of many computers, are cost effective in terms of their maintenance, demonstrate higher reliability since distributed systems do not have one single point of failure, and have the ability to grow organically (Drescher, 2017). A blockchain exists solely to achieve and maintain integrity in distributed systems by being a single source of truth for all the connected nodes.

Practically speaking, a blockchain is created as a secondary application of distributed peer-to-peer network running on top of the Internet. The most straightforward way to describe how the process of creating the blocks works in a simple, non-technical fashion was illustrated by Bashir (2017), where he explained:

> "blocks are accumulated when a node starts a transaction by signing it with its private key. The transaction is propagated by using gossip protocol, a protocol procedure where computers spread communication to peers. These computers communicate to disseminate information to validate the transaction based on

> the conditions agreed upon earlier by the network. Once the transaction is validated, it is included in a block, which is then spread to the network. The newly created block now becomes part of the ledger and the next block links itself cryptographically back to this block. This link is a hash pointer. At this stage, the transaction gets its second confirmation and the block gets its first. Transactions are then reconfirmed every time a new block is created".

This generic explanation of how blockchain works serves the specific purpose of understanding how it links to the features discussed previously and to qualify the disruptive nature of blockchains. There is also an entire parallel technical description of how the process of creating and maintaining a blockchain works, which goes beyond the scope of this dissertation.

It is important to highlight that blockchain has evolved since it was first created as core protocol of Bitcoin's initial implementation. As of 2017, there are three different generations. Blockchain 1.0 includes Bitcoin and all alternative cryptographic currencies. Blockchain 2.0 is an evolution of the blockchain protocol enabling not only exchange of transactions, but also programmes in the form of smart contracts that encode certain conditions and outcomes. This type is used to fulfil contractual agreements of legal contracts and define liabilities of the contracted parties or in asset protection, estate planning, and corporate governance. Lastly, blockchain 3.0 is used to implement applications beyond the financial services sector, and serves general-purpose industries such as government, health, media, the arts, and justice.

On the other hand, blockchain technologies have evolved in terms of the genre as well, and they can be classified at the moment of writing this dissertation into at least 10 different types; I will highlight only three in this section for the sake of simplicity: public blockchains, which are open to the public, where anyone can participate as a node in the decision-making process; private blockchains, which are open only to a consortium or a group of individuals or organizations that has decided to share the ledger among themselves; and lastly, semi-private blockchains where part of the blockchain is private and part of it is public (Bashir, 2017). The genesis and the open-ended nature of blockchain technology presents a basic idea about its potential to challenge the existence of a central authority entrusted with validating a process, an asset, or a transaction. This is because it is the only technology at the intersection between the database and network that allows saving and broadcasting the same reality to the participating nodes. In the case of blockchain, such nodes *are* the new authority.

This chapter provided a high-level definition of blockchain as a concept and a historical background of its origins. It also covered the main features of blockchain technologies, and

how the concept works to better understand the notion of trust and consensus building in a distributed network as opposed to having a central authority. The decision-making on blockchain occurs at the application level, which normally does not include or require a regulatory framework or any kind of interference from a third party – the traditional scenario in most if not all newly launched technologies, as every innovation has plenty of room to benefit from some level of autonomy until regulation catches up with it. The second chapter of this dissertation will address the role of regulation in deploying blockchain technologies, the policy and legal implications of these technologies, and how policy and regulation affects service delivery and economic relationships powered by blockchain technologies.

Chapter III

II. Blockchain applications: legal and policy implications

As of 2017, deploying blockchain technologies is not subject to regulation because any person anywhere in the world can create his/her own blockchain-powered application without the need to fulfil any regulatory obligations. The main reason for this vacuum is generally linked to the impracticality of regulating software where it is impossible to predict how it will be used. Moreover, the global accessibility and distributed nature of blockchain technologies trigger the questions of which jurisdiction will be regulating them? Which law applies, and how feasible it is to impose defensive regulation on a technology of which we are not yet aware of its full potential?

Regulation provides safeguards to investors and consumers, but it can also stifle innovation. The current approach to blockchain technologies varies as some countries are introducing specific regulatory and policy frameworks to promote innovation and growth, while preventing systemic risk, ensuring financial stability, and protecting consumers and entrepreneurs against economic harm and illegal activity. Other countries are not blinded by the promised economic boost or trust that government blockchains can generate, and have decided to ban it completely until adequate rules are introduced. This chapter will navigate the current regulatory framework specific to blockchain applications and their policy implications. It will also elaborate on the design criteria of blockchain technologies – namely open access, inclusiveness, and control distribution – and whether they could potentially replace the need of regulation.

2.1 Innovation versus regulating blockchain technologies

The adoption of blockchain technologies will revolutionise the Internet industry, business, and government services because, on the one hand, the concept and principles underpinning them respond to current social and political challenges, including transparency in decision-making, corruption, and abuse of power and authority. On the other hand, blockchain technologies motivate trust, efficiency, and quality of service, and they cannot be tampered with. Just like with previous inventions, however, every innovation triggers a debate about regulation. In fact,

the experience with blockchain feels like regulatory déjà vu, as the early days of the Internet generated the same concerns about how it should be governed, and whether or not it should be regulated using existing laws or left completely intact.

The Internet governance (IG) policy discourse encourages multi-stakeholder discussions with the aim to achieve a practical solution to governance issues pertaining to the Internet. Traditionally, the role of governments is magnified in the IG sphere, and even when the conversation is inclusive, the outcome does not always necessarily reflect the contribution of other stakeholders in policy implementation within a specific jurisdiction. It is important to note that the governance model of the Internet as an infrastructure is distributed among various organisations, which include but are not limited to: the Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for managing the Domain Name System, (DNS); Regional Internet registries (RIRs), responsible for the distribution of Internet Protocol (IP) addresses across the five regions of the globe; the Internet Engineering Task Force (IETF), which develops new Internet protocols; and finally, the World Wide Web Consortium (W3C), which is responsible for approving web standards such as HTML.

These organisations work in silos, can function without significant or visible interference from any government, and they all officially subscribe to common values, namely ensuring the Internet is accessible, open, secure, and resilient, but they also do not interfere in how a specific government regulates the Internet within its own jurisdiction. The Internet is an innovation that was equally challenging to regulators because no one could predict how it will be used. As soon as the Internet became a platform for business, however, trade law adapted to cater to transnational commercial operations. And when the Internet effectively became the new media, lawmakers and regulators in specific contexts classified expression regulation under cybercrime law, opted for applying existing laws to regulate content, and did not consider the uniqueness of the Internet.

Understanding the various layers under which the Internet operates could potentially help define a suitable model to blockchain regulation if required at all. An simple classification is provided by (Kurbalija, 2016), where he provides a simplified structure that links more than 50 specific issues to certain actors (e.g., organisations, governments, etc.), and divides the whole field of Internet governance into baskets, which coherently links infrastructure to protocols, applications, and content. The issue of regulation bisects all baskets due to the

complexity of the relationship between all the concerned stakeholders and the distributed nature of the Internet – a criterion that blockchain shares with the Internet. Nevertheless, it is expected that existing policies and regulation will need to be substantially adjusted to cater to new innovations – specifically something like digital currencies – in order to guarantee their legal stability as well as reduce the complexity of future digital policy regimes (Kurbalija, 2016).

Taking stock of the currently applied regulatory mechanisms on the Internet paves the way to measure their compatibility with the innovative nature of new Internet technologies. If we take into consideration the previous two examples on business and content regulation, the reality is trade law is not as comprehensive as necessary to solve the issue of tax evasion by technology companies, and the currently implemented Internet legislation on content triggers chilling effects on human rights, namely freedom of expression. If governments are to follow the same archaic rational to regulate blockchain technologies, the clash between innovation and regulation will persist since the essence of blockchain is code-generating, programmable logic, while regulation is usually broad and vague and, in many instances, does not fit the purpose of technological innovation.

The current regulatory trend of blockchain-powered products suggests that the approach many governments are taking is slow and cautious. Using cryptocurrencies as an example, regulating Bitcoin proved to be challenging because regulators struggled to classify it within the existing categories of financial products. In 2015, as Bitcoin's mainstream acceptability continued to grow, the Commodity Futures Trading Commission (CFTC) in the U.S. finally took the lead to classify it as a commodity since cryptocurrencies are still considered more of an investment than a way to pay for goods and services. "The CFTC mandate covers all forms of trades and bets made on the future performance of a commodity, regardless of what it may be, so by classifying cryptocurrencies under this umbrella term, it can apply its existing regulatory framework to the asset class" (Terekhova, 2017).

The European Union (EU) has yet to pass specific legislation relative to the status of Bitcoin as a currency, but the European Banking Authority (EBA) advised European banks not to deal in virtual currencies until a regulatory regime was in place (EBA, 2014). In fact, Bitcoin trading is legal in the EU, but it is yet not mainstream. Many services can be exchanged for Bitcoin and it can bought through few ATM machines; Europe tend to embrace innovation, which

positively impacts the perception about digital currencies Nevertheless, it is important to not overlook how the exponential value of Bitcoin throughout the more than eight years of its lifespan is pressing for more regulation.[17]

According to certain business analysts in the U.S., the regulatory uncertainty and the delay in introducing cryptocurrency rules is hindering the future growth of the sector and holding back investments of financial technology (fintech) firms (Terekhova, 2017). The same sentiment is shared in the United Kingdom, where it is believed that insufficient regulation could be holding back start-ups and the growth of fintech rather than creating opportunities through lack of regulatory constraints. In a recent interview with *The Telegraph*, Dr. Cathy Mulligan, co-director of Imperial College London's Centre for Cryptocurrency Research and Engineering, said, "Many start-ups in the U.K. are chasing the regulator to say, 'How are we going to be regulated?' rather than the other way [a]round" (Rees, 2017). Introducing regulation in this specific context particularly helps trading platforms seize the opportunity of bullish cryptocurrencies' market value that is entirely based on speculation.

The Japanese government's approach in this regard recognises the importance of legalising trading cryptocurrencies rather than allowing them to circulate in an unregulated environment. In September 2017, the Japanese Financial Services Authority (FSA) became the first regulator in the world to issue licenses authorising cryptocurrency exchanges (platforms offering trading options on cryptocurrencies such as Coinbase[18]), which legalises and regulates cryptocurrency trading and protects investors' interests (Young, 2017). The Japanese example teaches us that existing cryptocurrency regulation is narrow in scope and driven by quick gain from current market conditions. This is because it only focuses on legalising trading in Bitcoin and Ethereum and does not interfere with any other aspect of these cryptocurrencies, namely their value. Other recently published draft regulations, such as in Australia, are to include Bitcoin and cryptocurrency exchanges for the first time, but they mainly focus on anti-money laundering and counter-terrorism financing (AML/CTF) laws (Das, 2017).

The current trend of cryptocurrency regulation is not representative of governments' perception about how blockchain technologies should be regulated. It is important to note the increasing interest from governments in distributed ledger technology (DLT) as an open, secure, scalable, transparent way to imbue transactions with trust and confidence. As a result, several regulatory

[17] As of February 2018, 1 Bitcoin equalled $7,639 vs. $0.16 in 2010 – a 4,774,375 per cent increase in value, but far lower than its high of $20,000 at one point in December 2017. For the latest price, see: https://www.coindesk.com/price/.
[18] https://coinbase.com/.

bodies are forming taskforces and working groups to identify the capabilities of blockchain technologies since they are keen to promote technology that lowers costs and increases transparency (Bear, 2017). This could indicate a change in the regulatory landscape pattern where lawmakers have no choice but to let the market decide the rules.

Generally speaking, regulators are not often viewed as innovative or particularly concerned by innovation (Bear, 2017). In the case of blockchain, however, they are increasingly proactive in testing how it can reduce systemic risk usually triggered by the lack of efficiency and transparency in handling business operations. Having said that, DLT and especially smart contracts are under scrutiny by governments with the rise of initial coin offerings (ICOs) (see page 46 for more information on ICOs).[19] Further elaboration on this specific point will be covered later in this chapter when analysing the existing regulatory frameworks applicable to smart contracts. The next section will focus on the policy implications of blockchain applications and to what extent such policies affect their deployment.

2.1.1 Policy implications of blockchain applications

Disruptive technologies like blockchain often foster creative solutions to key industries and catalyse economic transformation. Yet, in the wake of technological innovation, the theory and practice of public policy is frequently confronted with a corresponding challenge to develop fact-based research, which establishes the impact of the technology in question on public policy. There is no doubt that the affordances of the technology have outpaced the regulatory capacities of law and legislation, which prompts a close examination of current public policy approaches to establish if they are sufficient or if there is a need to catalyse new thinking. Blockchain-powered applications could be the most important emerging technological trend to shape public policy. Nevertheless, there is a research deficit that defines the policy challenges of this technology as a key emerging issue in public policy. Therefore, it is vital to understand if the existing policy ecosystem caters to such technology, and if the current approaches and regulations can be applied.

One the most highlighted policy issues in the Internet era is privacy, and it is no different for blockchain technologies to trigger the same concerns. The discussions revolve around the

[19] An ICO is a fundraising mechanism in which new projects sell their underlying crypto tokens in exchange for Bitcoin and Ether. See: http://www.nasdaq.com/article/what-is-an-ico-cm830484.

impact of blockchain technologies on privacy, especially public ones such as Bitcoin or Ethereum, where the PoW process sometimes requires personal data to verify if the data added on the blockchain is valid and transparently stored to avoid fraud by rogue nodes. In essence, public blockchains are permissionless, and anyone in the world can initiate and participate in processing transactions. Thus, ultimately ensuring the credibility of an exchange in a trustless environment was deemed much more important than the notion of privacy.

Buterin (2016) admitted that privacy on blockchains is a pressing matter, but not more important than the scalability issues. He asserted that when "blockchains are being used to build data-centric systems or applications, where users are in control of their own data, these blockchains do not solve privacy issues, and are an authenticity solution only." In order to secure this data, Buterin thinks that other technologies that offer privacy, such as encryption, can be utilised in order to create a holistic solution for many industries, where blockchains can be solely treated as vendor-neutral platforms where some data can be stored to provide authenticity guarantees.

The issue of blockchain privacy prompted developers to identify suitable solutions because it can hamper its adoption. The current trend suggests that ensuring privacy by design on private blockchain applications is doable by applying new techniques to hide the values of a transaction and the asset itself. Participants of the blockchain can still prove that the transaction adds up, but they do not know the amounts or the type of assets being exchanged (Blockstream, 2017). These schemes also enable both confidential and non-confidential assets to co-exist on a single blockchain, and allow for selective disclosure of private data to designated third parties (Andreev, 2017). In this case, it makes privacy an inherent feature on the blockchain, compatible with programs, and dependent on established cryptographic primitives that allow for their performance to be optimised and scaled. These techniques have implementation limitations, however. For example, confidential transaction implementation only hides a certain number of the digits of the amount of each transaction output (The Elements Project, n.d.). There is a confidential minimum and a maximum amount, and any smaller or larger amounts than the minimum and maximum are revealed to observers, which allows them to follow and link the transactions with identical amounts in order to reveal the order of amounts' magnitude.

Developers are also exploring techniques such as obfuscation using cryptography, which allows "users to benefit from the security of a blockchain, using a decentralized network to process the transactions, but 'encrypting' the data in such a way that even though everything is being computed in plain sight, the underlying 'meaning' of the information is completely obfuscated" (Buterin, 2016). Each of the presented solutions to privacy on the blockchain has its own limitations, but there is a continuous effort by the blockchain developer communities to devise suitable technical solutions to address emerging issues. Nevertheless, it is extremely challenging to predict the full impact of blockchains on privacy without assessment, which explains why blockchain developers engage in open discussions with the wider community about the applicability of the theories they adopt in solving blockchain's limitations. The discourse usually triggers several revisions of the code and further testing to the proof of concept. It is likely that only after deploying blockchain applications, however, will a holistic view on their impact and limitations manifest since the final product in technology is always a work in progress.

Security is another policy issue hindering the scalability of blockchain technologies, even though the various industries described previously are exploring their potential and how they can be incorporated into their business model. It is unlikely that public blockchains are appealing to large organisations due to the complexity around encryption key management and the cryptographic processes of transferring assets or data on a blockchain. The participating nodes on public blockchains usually store and generate encryption keys via software-based programmes, which means they are vulnerable to both physical and virtual theft. The encrypted data is then no more secure and can be easily compromised (Rome, 2017). Large technology companies are prompted to mitigate security vulnerabilities by adopting secured and compliant cryptographic operations for key management, storage, and other cryptographic operations. However, adhering to government security standards cannot guarantee physical theft of storage or virtual attacks will not occur.

Security concerns on public blockchains extend to other issues as well, such as stability and the efficacy of the platform, which can be intimidating to companies willing to use a blockchain-based system to increase their transparency. That is why private blockchains offer a degree of control over both participant behaviour and the transaction verification process. They allow the early consideration of the system's security integrity starting with the network architecture to ensure the nodes transmitting information are genuine, accountable, and easily

traceable – ensuring robust verification of transactions in a relatively shorter time span compared to public blockchains (Berke, 2017).

Today, the security and privacy properties of blockchain technologies are still emerging fields that require extensive research and concept proofing. Bitcoin's core technology, blockchain, was initially introduced as a practical mechanism for a permissionless, decentralized, and tamper-proof digital currency. The core features of Bitcoin, however, namely its public verifiability, do not provide the security and privacy properties assumed by its users. "For example, despite a common assumption that Bitcoin is anonymous, transactions can be de-anonymized, limiting the commercial utility of the network and also harms individual privacy. Generalisations of Bitcoin's underlying blockchain technology as a platform for smart contracts by Ethereum are still immature. For example, security issues in the underlying programming language for smart contracts in Ethereum led to the massive DAO hack. More than ever, proper security and privacy properties need to be designed into the underlying framework for blockchain technologies" (Buterin, 2017).

The scope of blockchain deployment extends to include future innovations that are still in the testing phase, such as artificial intelligence (AI). For example, a start-up in the U.K. (colony.io) has developed a platform for individuals to collaborate on large-scale projects called colonies or enterprises. It uses Ethereum's smart contract system to track collaborations and reputation, manage productivity, and transact payments using their own cryptocurrency. "By building colonies, contributors collect unique tokens, which serve as "proof of cognition," and can be traded on the open market for cash. The company uses AI to analyse contributions and reputation to direct the right project listings to the most appropriate talent at the most opportune time" (Groopman, 2017). In this regard, privacy and security considerations on blockchains are prerequisites to keep pace with the emerging trend of software-combining artificial intelligence (A.I.) with blockchain technology to bring trust and security in using AI-driven autonomous agents. It will be significantly challenging to predict a stable operational environment, which practically fills the gaps of existing exchange applications such as application programming interfaces (APIs), but does not adhere to standardisation principles or comply with regulation simply because they do not yet exist. Yet, the International Telecommunication Union (ITU) is leading a discussion on standardisation. A recently formed ITU focus group on blockchain and distributed ledger technology platforms will be working on identifying and analysing DLT-based applications, best practices, and guidance, which supports the implementation of those

applications on a global scale, and defines a way forward for related standardisation work led by other ITU Study Groups.[20] The focus group will then develop a standardisation roadmap for interoperable DLT-based services, which support a broad set of applications across many domains.

The importance of standardisation emanates from the fact that it produces policies that prevents market dominance by a single application and ensures equal recognition of a specific product and related platforms. Standardisation ensures that all forms of a specific technology are treated equally in policy implementation and regulation. In the case of blockchain technologies and DLTs, standardisation could mean that these platforms are to be considered the same as other technologies from legal and liability perspectives. Therefore, blockchain operators and developers can rely on a unified framework to conduct their business. Nevertheless, standardisation has its own limitation since it is challenged by market dynamism, and does not necessarily cater for innovative solutions addressing emerging issues.

In sum, there is a set of policy challenges that should be addressed for blockchain technologies to thrive, namely those addressing privacy and security. Blockchain technologies are more appealing as a concept than their practical deployment, and defining a regulatory framework for them to function will play a key role in their legitimacy to operate. The next section will focus the current legal and regulatory considerations to blockchain deployments and how they fit into the current legal landscape.

2.2 Legal and regulatory challenges to blockchain deployment

The core technology of public blockchain applications being permissionless and trustless poses legal and regulatory challenges because of the ambiguity around the contractual effects of smart contracts. While standard agreements can define the legal relationship between the parties involved, it is not clear yet how the existing regulatory frameworks cater for transactions conducted on the blockchain. The transnational nature of these contracts also triggers plausible jurisdiction conflicts that extend to include users, third-party providers, and blockchain application operators. Managing the complexity of legal relationships and liabilities among these parties is an understatement when the whole filed is currently operating in the absence of

[20] Members of the public are free to join the working group. See: http://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx.

formal contracts. Parties currently participating in blockchain deployments and transactions run the risk of uncertainty because of the lack of clarity around the existence of a contract and its terms.

The issue of jurisdiction intensifies with the realization that the nodes on a blockchain can be located anywhere in the world. Careful consideration of contractual relationships in a blockchain network will be required to fulfil the requirements of contracts and titles across jurisdictions. Identifying the applicable jurisdiction in a decentralised environment will be evidently challenging because defining and applying the appropriate governing law will be essential to guarantee legal protection.

There are various ways to envisage which jurisdiction could potentially apply to transactions on the blockchain. The least practical would be to consider tracking the location of each and every node in the network to define the applicable rules. Clearly, this could result in the blockchain needing to be compliant with an unwieldy number of legal and regulatory regimes (NortonRoseFulbright, 2016), and would require accuracy pinpointing to the location of the transaction within the blockchain. That aspect in particular could be challenging if a node is using a proxy server to access the Internet. Assuming that blockchain technologies operate under specific contractual agreements (they are not at the moment), existing legal systems could solve this dilemma by including the governing law to be applied, which determines the rights and obligations of the parties to the agreement and which courts will handle any disputes (NortonRoseFulbright, 2016).

In this regard, the licensing and regulation of blockchain technologies could play a key role to solve these legal dilemmas, but this solution will require standardised procedures and streamlined process that cater to transnational legal relationships. A number of jurisdictions are working on setting up a regulatory framework to attract blockchain start-ups since investments in this emerging technology are soaring. Gibraltar's financial services were the world's first to issue a bespoke blockchain license by the end of 2017, followed by Malta. The licensing concerns all companies using DLTs, but it primarily targets financial services since both jurisdictions are very experienced in handling financial products. It is not clear yet how these licenses will be implemented on other blockchain products or how they will address the complexity of legal arrangements. Their purpose appears to be more geared towards attracting investments and perhaps to be at the forefront of regulation.

The legal industry expects a number of liability issues to deploying blockchain technologies. The absence of defined contractual parameters exchanging value over a blockchain exposes adopters to the risk of uncapped liability and counterparty risk. While it is possible to impose specific conditions of admission on participants of permissioned systems – for example, by ensuring they fully comply with standard procedures such as know your client and anti-money laundering requirements (KYC-AML) – it will be quasi-impossible to apply the same rules on permissionless systems because anyone can participate in a blockchain without going through compliance procedures. In this case, more innovative solutions need to be identified to ensure parties can be held liable if and when the need arises.

Liability issues are usually addressed from the legal perspective by defining the applicable consensus protocol to determine the current state. The contractual status relating to participation in a blockchain deployment should therefore be ascertained during the use case for the technology and agreed upon prior to launching the product (McKinlay et al., 2017). An administrator could be appointed to vet the system; in the case of consensus, participants commit to provide node processing to define liability issues within the blockchain application (NortonRoseFulbright, 2016). This solution indicates that human intervention is indispensable to enforce the rules as well as impractical; the whole purpose of blockchain is to omit the middleman.

The current legal advice provided by law firms prognosticating on blockchain legal issues propose that businesses set up an arrangement to include provisions that consider trust boundaries in governance arrangements between the participants. A trust boundary is "the place where the ledger integrates with anything that is not in the ledger, such as onboarding trusted entities as ledger members, or entitling an entity to issue an asset into the ledger and validating that the rights to the specific asset are owned by that entity, and that those assets are properly secured off the ledger" (McKinlay et al., 2017). This setup suggests that a record constituted by a blockchain can reflect a transfer of an asset for value. This arrangement is similar, to a large extent, to the governance structure of financial products namely securities which are normally regulated via a local financial authority. The legal advice provided to blockchain operated businesses and clients also includes a clear stipulation of technical requirements, namely service levels for latency, bandwidth, and software updates to minimise disruption as well as improve performance. Other requirements focus on risk allocation relating to the liability for faulty systems resulting in transaction failure and termination rights (NortonRoseFulbright, 2016). The legal provisions related to establishing contractual

agreements of transactions conducted across a blockchain should be as specific as possible. The precision of what terms apply to a transaction will mitigate any loopholes in the system that could change the legal relations between participants.

Resolving disputes involving blockchain products and smart contracts specifically can be problematic in a number of jurisdictions if the legal requirements of a contract are not fulfilled. This primarily includes the legal capacity to enter a contract, the common law authority that decides the contract is binding, and the availability of sufficient information about the other contracting party or parties. Due to the distributed nature of how smart contracts operate, building consensus within the network only focus on verifying the authenticity of the transaction. Hence, the power of decision is in the hands of scattered nodes, and there may be no central administering authority to decide on a dispute between participants.

Legally speaking, there may simply be no obvious defendant against whom legal action could be brought vis-à-vis blockchain technology-related disputes, which makes litigation and dispute resolution complicated if not impossible. Seeking legal redress for breach of contract in court requires the participants to be legally defined as well as proof that a contract exists between participants in the first place. Knowing that blockchain transactions are presumably anonymous and no contract is in place could mean a court will be unlikely to consider a smart contract hosted on a blockchain legally binding if it is not possible to identify who the other contracting party or parties are (NortonRoseFulbright, 2016). The current legal practices and dispute resolution mechanisms suggest that enforcing a court judgment or arbitration in respect of a transaction using blockchain technologies is ambiguous and not straightforward. The level of complexity will eventually increase as blockchain technologies evolve and start interacting with third-party systems.

Transacting online comes with a sheer number of considerations because the existing systems, whether legal or regulatory, are challenged by the robust and transnational nature of technology in general. Another predictable issue following the widespread of blockchain transactions is taxation. Regulators need to persevere to define suitable mechanisms to facilitate international allocation of taxing rights. Traditionally, tax regimes are tied to the place where contracts are concluded. As stressed, however, blockchain technologies thrive on the very notion of decentralisation, which presents yet another challenge to conventional tax systems.

Finally, blockchain technologies will give rise to a number of intellectual property issues, which include:

- Patentability;
- The use of trade secret protections in relation to component parts of the technology constituting a blockchain system, including algorithms, databases, software;
- Infringement risk associated with the use of the technology; and
- The impact of the use of open-source software in blockchain technologies.

Other key issues include the applicability of laws regulating digital signatures, various cybersecurity considerations, and the legal effect of bugs in blockchain systems, transactions, or the programmable logic included within a message or a block.

The ethos of blockchain technologies is practically agnostic to existing legal and regulatory frameworks because the entire concept evolves around building a reputation in a trustless environment that completely avoids the judgment of a centralised authority. Scaling the concept and applying it to business operations, however, shifts our attention to protection mechanisms to safeguard property rights if and when undue circumstances arise. Hence, the focus on the legal identity of blockchain participants is of utmost importance to define liabilities.

There is currently a discussion to define the intersection between legal and technical code to shape regulatory frameworks by combining both to ensure blockchain technologies comply with legal rules. Nevertheless, the concept of "code is law" is not new and was originally introduced by Lawrence Lessig in one of the pioneering publications about Internet regulation. Lessig (2006) asserted that "law is in the original code," which suggests that programmable logic could be used to implement the legal code. Theoretically and technically speaking, this step would solve many of the legal and regulatory issues in the technology field. In practical terms, however, decentralised technologies – such as AI, the Internet of things (IoT), and blockchain applications – are currently being developed in silos, away from eyes of regulators, and are driven by market demand. They rather align with the industry ownership of the technology they develop to maximise their benefits than comply with regulation.

Innovation is generally intimidating to lawmakers, and technology never fails to outpace regulation. Blockchain technologies and smart contracts pose new complications, though, which is not only challenging to existing regulatory frameworks, but also to the concept of regulation itself. Blockchain challenges the status quo, stipulating the rules and promises to restore decision-making powers back to the masses. This, however, is much easier said than done because regulation is inevitably catching up with the hype around blockchain. The next

paragraph will dive into exploring the extent to which existing regulatory frameworks interact with blockchain technology deployment.

2.2.1 Regulatory frameworks' compatibility with blockchain technology deployments

The rise of blockchain as a concept beyond Bitcoin is appealing because it holds the promise of circumventing centralised authority in decision-making, reinforcing transparency and trust in systems in general, and most importantly, it is considered a step forward to establishing a true peer-to-peer sharing economy. This line of thinking is made possible because of the genius behind Ethereum, the second-largest and fast-growing blockchain application (Tapscott and Tapscott, 2016) and the issuer of Ether, a cryptocurrency that rewards the initial supporters called miners – individuals or groups who invest energy through their computers to solve complex cryptographic puzzles to secure the network by verifying and validating the blocks on the chain. In turn, the miners are rewarded with cryptocurrency for the computational effort they spend.

Ether is a digital asset that can be compared to a security or a bond for the sake of simplicity. Instead of operating as a digital currency, Ether is used to provide fuel to pay for the computational effort to execute contracts on Ethereum's network. Just like a car needs fuel, Ethereum does too via Ether. For example, assume that a smart contract is created on Ethereum to set up a decentralised online academic journal. To post, delete, or modify an article, you need to pay a transaction fee in Ether to get the network to process the change.

Ethereum is a platform that runs decentralized applications commonly known as smart contracts. As Ethereum's website states, this technology "provides powerful tools to help developers create software and applications on a custom-built blockchain infrastructure that can move value and represent the ownership of a property." This includes the option "to develop an Ethereum-built smart wallet that holds and stores cryptocurrencies, the possibility to design and issue one's own cryptocurrency by generating tradable digital tokens that can be used as a representation of an asset or a virtual share." Finally, Ethereum offers a platform for kick-starters to convene trustless fundraising events to develop their ideas, which constitutes a turning point in the mainstreaming of blockchain applications.

Ethereum is the first blockchain application that introduced a Turing-complete language and the concept of a virtual machine. This opens endless possibilities for the development of

decentralized applications, and provides a public blockchain to develop smart contracts (Bashir, 2017). After its launch in 2014, the number of new Ethereum-powered applications mushroomed in a very short timeframe and so did the crowd sales events commonly referred to as initial coin offerings (ICOs), a fundraising mechanism that allows new projects hosted on the Ethereum blockchain to gather the capital needed to further develop their concept by selling their underlying crypto tokens in exchange for Bitcoin and Ether. In principal, this funding model resembles an initial public offering (IPO), where a private company offers shares to the public to increase their capital, except that an ICO is rather an investment in the potential of a concept becoming the next big business venture that could generate millions in revenue. Financial analysts have rang alarm bells that such investments in products which do not yet exist is extremely speculative and risky (NASDAQ, 2017). Another way to look at it, though, is that this fundraising style is an innovative way to incentivize protocol customization according to the needs of the market since the ICO participants can have a say in how the product is shaped.

The ICO phenomenon caught everyone off guard including regulators. Since the fourth quarter of 2016, $3.3 billion has been raised in more than 200 ICOs, and without any obstruction from regulators (The Economist, 2017). Thousands of projects were created that launched their own ICO by creating a smart contract on Ethereum to provide contributors with the possibility to purchase the cryptocurrency derivative of the product in question. ICOs are set to run for a specific timeframe or until a goal is reached. “Depending on the outcome, the funds will either be released to the project owners or safely returned back to the contributors. All of this is possible without requiring a centralized arbitrator, clearing house, or having to trust anyone. You can even use the token you created earlier to keep track of the distribution of rewards” (Ethereum Project, 2017).

Until around the middle of 2017, there was no clarity if ICOs are legal or not, or if their classification falls under a specific asset category. “In some cases, the token is simply a utility token [that] gives the owner access to a specific protocol or network; thus, it may not be classified as a financial security. On the other hand, if the token is an equity token, meaning that its only purpose is to appreciate in value, then it looks a lot more like a security” (NASDAQ, 2017). Regulators in the U.S. represented by the Securities and Exchange Commission (SEC) have found it harder to fit cryptocurrencies into their current taxonomy (Terekhova, 2017). Nonetheless, they finally reached a decision on regulating ICOs by

announcing in late July 2017 that that virtual tokens are securities, and are now subject to federal securities laws (Akhtar, 2017).

The SEC decision opened the door for other countries to impose similar rules. For example, United Arab Emirates (UAE) decided to provide guidance on the regulation of issuing new cryptocurrency through ICOs by stipulating how they will categorise issuing tokens.[21] They identified three categories that the regulation covers: security offerings are restricted to accredited investors; issued cryptocurrencies are to belong to a regulated entity that would have to adhere to anti-money laundering laws; and crypto-derivative services that would be required to abide by regulated Clearing Houses and Recognised Exchange infrastructure (Bitlegal, 2017). Other countries have addressed cryptocurrency regulation as well, such as Gibraltar and Malta (as mentioned previously), as well as Russia and China. Gibraltar announced they will be regulating ICOs and blockchain-based applications, but their plan it is not exactly clear.[22] Russia, on the other hand, mandated new regulations around cryptocurrencies in 2017,[23] while China chocked the cryptocurrency community by making a bold move to ban ICOs and Bitcoin altogether – an expected move that is "drastic but understandable and reasonable, and like the market reaction, probably temporary" (Acheson, 2017a).

It is evident that both the markets and regulators were not prepared to deal with the ICO boom. The compatibility of current regulatory frameworks with the robust nature of smart contracts will be put to test if the developers of this technology devise solutions against existing regulation of activities. The market will dictate if the current classification of ICOs as a financial security will foster migration to blockchain technologies. After all, we already know that ICOs flourished in the absence of regulation, which means that the market has decided to put its faith in this concept, and, undoubtedly, the underlying principles of blockchain technologies are the main driver of this growth. We are yet to witness if this early wave of regulation will guarantee a reasonable level of security anticipated by investors, however.

Regulators, on the other hand, are not oblivious to the innovative opportunities arising in unregulated areas, and are aware that wiggle room ought to be allocated to accommodate this

[21] https://www.adgm.com/media/192772/20171009-fsra-guidance-for-icos-and-virtual-currencies.pdf.
[22] http://bitlegal.io/2017/05/09/gibraltar-issues-new-blockchain-regulations/.
[23] https://www.coindesk.com/vladimir-putin-mandates-new-rules-cryptocurrencies-icos/.

kind of technology. The EU and UAE[24] appear to be following this path by adopting an innovation-first philosophy, allowing the exploration of use cases to test impact and laws, and gives entrepreneurs confidence that their approved applications will be more trusted by their target markets (Acheson, 2017a). Shedding defensive regulation in favour of a more supportive approach could change the perception that businesses and citizens have of their government, and could even be able to help resurrect trust in public institutions.

Beginning in 2018, blockchain technologies will also need to comply with the EU's General Data Protection Regulation (GDPR), which comes into effect in May, and replaces the 1995 Data Protection Directive.[25] GDPR is specifically crafted to deal with centralised models of companies utilising personal data in ways that compromise individual privacy. The new regulation also addresses centralized models of digital data storage and transmission that are now in the process of being replaced by blockchain technologies, where the users are the primary owner of their data (Smolenski, 2017). This logic is in line with GDPR[26] and its goal of empowering users to be in full control of their personal data. Yet, to ensure compatibility with the new legislation, some of the core features of blockchain technologies ought to fulfil other requirements of the new regulation, namely Article 17,[27] Article 18,[28] and Article 22.[29]

The approach taken towards blockchain regulation by the governments mentioned as well as others varies according to a number of factors that transcend economic benefits, especially in countries like China. Some analysts have hinted that the ICO ban in China is motivated by the urge to maintain social balance and stability in the wake of the "get-rich-quick mentality," even though the statement issued by The People's Bank of China (PBC) labels token sales as "illegal and disruptive to economic and financial stability" (Acheson, 2017b). Other approaches, such as EU's, leans towards encouraging an ecosystem of thinkers and doers to boost the economy and to become a frontrunner in blockchain innovation. This rational leaves plenty of room to test the boundaries of legality and policy, and allows for experimentation vis-à-vis how to apply regulatory limits on a hybrid asset that mixes between offering a product powered by blockchain as well as a financial product in the form of a cryptocurrency that gives its shareholders the power to decide how the product will be developed. Yet, such a model also

[24] The supplementary guidance document issued by the financial services authority of UAE invites issuers to engage with the regulator as early as possible to collaborate and to identify suitable regulatory mechanisms.
[25] http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.
[26] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.
[27] **Article 17:** The right to have personal data erased when they are no longer necessary for the purposes for which they were collected and there is no legal ground for their maintenance.
[28] **Article 18:** The right to restrict data processing where the data is inaccurate, its collection unlawful, or its processing no longer required.
[29] **Article 22:** The right to not be subject to legal outcomes that rely solely on automated data processing.

triggers a new dilemma of how to manage soft power accumulation in distributed governance in addition to the previously highlighted policy and regulatory challenges.

This section offered a close examination of some examples from currently implemented regulatory frameworks, how they apply to blockchain technologies, and the potential limitations vis-à-vis GDPR deployment. The next section focuses on analysing the design criteria of blockchain technologies, and how they do or do not comply with the future of regulation.

2.3.2 Blockchains design criteria and regulation

Blockchain technologies advocate for open access, inclusiveness, and control distribution in the decision-making by design, but there are several hurdles to their mainstream adoption from the technical standpoint. Specifically, this includes when the scalability and the efficiency of the technology are questioned with the growing number of proof of concepts exposing technical vulnerabilities. The electricity cost to mine one Bitcoin, for instance, amounts to around $26,170,[30] according to a report by Elite Fixture (Goenka, 2018), and the most – if not only – sustainable solution defined so far is by Dutch researchers who are using body heat to mine Bitcoin (Redman, 2018). Developers, on the other hand, are racing to address the scalability issue because it could hamper the adoption of blockchain technologies, and potentially influence public opinion and the buy-in of the concept. Therefore, technological advancement in this area is entrusted with finding a suitable solution to such limitations. But what happens when the core design criteria of blockchain technologies do not fulfil the requirements of currently implemented regulation or planned regulation such as GDPR?

The immutability criterion of blockchain technologies is instrumental to achieving the highest levels of transparency, and is promoted as a core feature of the technology. The concept, however, came under scrutiny following the hard fork incidents of the DAO and Bitcoin. The move was decided by the core developers to mitigate a hack that would have been damaging to the value and credibility of these products and to maintain the integrity of the network. The hard fork is a radical change to the protocol to annul the invalid generated transactions resulting from attacks or theft, but they can also be implemented to introduce a protocol software upgrade. Strangely enough, such action was not of concern to regulators because these products

[30] The price list of electricity for Bitcoin mining indicates that the highest cost is registered in South Korea and the lowest in Venezuela. For more information, see: https://businesstech.co.za/news/banking/221837/the-cost-of-mining-bitcoin-in-south-africa-vs-other-countries/.

are unregulated. Instead, it is the community of miners behind these two products who resisted the hard fork due to conflicting interests (Breitman, 2017). Nevertheless, researchers question blockchain's immutability concept because the inability to remove information can trigger an issue vis-à-vis the implemented regulation.

Blockchain technologies are perceived to hamper information privacy because of the immutability of the data processed. As a result, it is complicated for law enforcement to apply so-called Right to be Forgotten regulation within the EU, for instance, since blockchain technologies rely on a distributed data storage system where its entire node network records the same information and change requires the majority of the network to agree (Gabission, 2017). Moreover, such a change would also require the availability of powerful computational resources. The data saved on a blockchain will have to comply with data protection regulation, except that the current mechanisms – and even the new GDPR – are conceived to address centralised business models handling sensitive data, while blockchain technologies are decentralised in nature.

In a centralized system, a judge can request that the central server take down information in breach of the user's right to privacy. Whereas in a decentralized system, "Multiple nodes carry identical copies of the same information – nodes that may not even be within a court's jurisdiction. Enforcing a takedown of information becomes complicated if not impossible. If unwanted information gets on a blockchain, it may have to continue to exist in order to protect the integrity of the overall system" (Tennison, 2016). In a similar context, some recently launched applications mobilise blockchain technologies to circumvent censorship. In such a system, defamatory statements could live beyond the original posting into permanency and can be downloaded or disseminated again (Gabission, 2017). Policy-makers need to pay attention to this issue even within the current state of technology, and how all the above examples interfere with the universal right to free expression.

It is believed that copyrighted work could end up unlawfully on a blockchain. Once recorded on the ledger, it will be impossible to take down the materials because no central server can be disconnected, but it is certainly possible to track it down throughout the network. As discussed previously, the participating nodes hold the responsibility of the network's integrity, and the legitimacy of assets is a perquisite as a principle. Gabission (2017) asserted that when copyrighted work ends up on a blockchain, they must decide from whom to collect royalties following the current system, which gives them the right to pursue compensation from the

facilitating parties or intermediaries as stipulated in the Digital Millennium Copyright Act (DMCA), the currently implemented regulation and a principle tool for online copyright enforcement in the U.S. There is a counter narrative, however, as to how blockchain technologies can facilitate exercising copyrights more efficiently by applying a "Uniform Commercial Code to do online what the code had already expedited in physical space" (Tapscott and Tapscott, 2016b). The proof of work mechanism on a blockchain defines ownership of every asset, for instance, which prevents unauthorised trading in real property, intellectual property, or rights of personhood.

Copyright holders can make use of blockchain to prove ownership of their work, enforce contractual rights, and oversee implementation, which was previously unattainable over the Internet. Blockchain's smart contracts can handle more complex transactions involving bundles of rights and multiple parties. This piece of special purpose code has the ability to execute a complex set of instructions. "That intersection of legal descriptions and software is fundamental, and the smart contracts are the first step in that direction," Steve Omohundro, president of the Self-Aware Systems think tank, said (quoted in Tapscott and Tapscott, 2016a). A smart contract provides a means for copyright holders to have full control over their work by assigning usage rights to a contracted party, and they can also specify the properties in the code of the contract to include the terms, duration, termination, and penalties.

Smart contracts are innovative in providing a means for owners of assets to code their resources into the contract that clearly underpins and enforces their rights. It is an unprecedented method of ensuring contractual compliance, but it will require initial investments to guarantee long-lasting impact on economies in general. Once blockchain technologies are fully mastered at a large scale, the legal and regulatory issues will likely be addressed at the periphery of its implementation. This is because the focus should be on how blockchain technologies complement what the Internet cannot do, not on how the design criteria of such technologies contradicts currently implemented regulation. Ultimately, DLTs and smart contracts emerged in challenging policy and regulatory ecosystems, as the offline world is still coping with and adapting to the social, economic, cultural, and political shake-up triggered by the Internet. What started as an exchange protocol to transfer information in a closed research network has evolved to create an everlasting impact on every aspect of our daily lives.

To conclude, identifying the legal and regulatory challenges of blockchain technologies requires deep understanding of how this technology works. The applicability of blockchain

principles is partially tested, and most of the products are still in the proof of concept stage. It is perhaps more crucial to closely examine the inclusiveness and control distribution within blockchains, and how soft power accumulation manifests in distributed structures. The next chapter will focus on elaborating on these specific points, how they link directly to the governance structures of blockchains, reasons why they should be trusted, and how they can have a pivotal role in defining the legitimacy of blockchain technologies.

Chapter IV

3.1 The governance structure of blockchains

The rise of blockchain and distributed ledger technologies has prompted a debate about how they are governed, as well as how the decision-making of the protocol defining the rules in these blockchains is agreed-upon, created, and modified. Governing decentralised systems is multi-layered and does not adhere to the standard governance principles, which do not necessarily have a positive connotation. Existing governance mechanisms are centralised in nature, and can be easily manipulated through lobbying; their existence could be a mere compliance procedure when the decision power remains within a closed circle minority. Blockchain technologies gain their integrity from a set of rigid rules depending on consensus of various stakeholders influencing their direction. The governance debate should not be specific only to blockchain protocols, but it also extends to include the "system's ability to adapt in the face of technical challenges, evolving use cases, and ideological differences" (Wang, 2017).

Permissionless blockchain technologies' governance model is subject to scrutiny because their implementation is challenged by scalability limitations, the identified vulnerabilities of the DAO, and hacking incidents of Ethereum[31] and Bitcoin.[32] The hard fork events are usually criticised because they contradict the immutability feature of blockchain, and they trigger a divide among the communities supporting or developing them. Having said that, hard fork events are also organised to introduce improvements to the underlying protocol and obviously to address the vulnerabilities just like any other software products.

Without having a credible governance mechanism, blockchain technologies might not live up to their promise to address the growing deficit of accountability and trust in both public and private institutions. A credible governance mechanism is also required to improve existing governance structures by providing new opportunities to establish a new operational layer for

[31] The latest hack drained $32 million in Ether (see: https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce). Other incidents involve locking down funds and hacking exchangers wallets.
[32] There have been many incidents over the past five years where millions worth of Bitcoins were stolen from exchangers or wallets. The overall value of the hacks is defined according to the market price. See: https://www.benzinga.com/fintech/17/11/10824764/the-11-biggest-cryptocurrency-hacks-in-history.

human interaction that can support, complement, and perhaps even replace current governance structures.

The governance structure of blockchain technologies can be illustrated by examining the models of the two widely used blockchain applications: Bitcoin and Ethereum. Both are software-run cryptocurrencies that are high in value, and subsequently target to attacks and, in some cases, legitimate actions to siphon funds. Finally, they both organised hard fork events that can serve as a guide point to their methodology in building consensus among the various stakeholders involved in the decision-making process.

Satoshi's Bitcoin protocol comprises a set of rules in the form of distributed computation operations that ensured the integrity of the data exchanged among devices without passing through a trusted third-party (Tapscott and Tapscott, 2017). Bitcoin's protocol was established as a system involving checks and balances between three different stakeholders: developers, miners, and users. Any changes to the code and economics of Bitcoin require the participation of all three stakeholders to be implemented. Developers write the software that runs on the protocol, but miners and users must vote for the software by running it themselves (Tomaino, 2017). It is in the interest of all stakeholders in this community that the chain is transparently formed by genuine blocks because it is a decisive factor in building trust among the network – and vital to defining and maintaining Bitcoin's value. Therefore, it is safe to state that the governance structure of Bitcoin is incentivised because everyone owns the responsibility to maintain the integrity of the code and will be rewarded for their role in the chain. It raises key questions, though, such as how do we incentivise the public, outside the Bitcoin community, to trust an unconventional governance structure, and is the current governance model of Bitcoin efficient in the long-term?

Before answering these questions, it is worth elaborating first on the concept of checks and balances that Bitcoin follows. In theory, it might have been inspired by the traditional democratic values of a political system, which dictate separating the judiciary, the legislative powers, and the executive powers. Therefore, governance is implemented at the institutional level, and always requires a central focal point to guide decisions. In the case of Bitcoin, consensus over protocol development is distributed among the previously defined stakeholders. Satoshi's absence, however, means that there is no single authority tantamount to an executive president or prime minister to exert its power to decide the rules of the protocol or to guide the community. Satoshi's rational was to align stakeholders' incentives through the code itself, and

the technology thrived in its early years, blossoming into the ecosystem we know today (Tapscott and Tapscott, 2017). But then he disappeared, and every decision to implement any changes to the protocol is left to the core developers. No person or group in the Bitcoin community has significant influence on the developers, users, and miners (Tomaino, 2017), which could be the reason why Bitcoin has not made any major protocol changes to improve its scalability. Bitcoin's core development team requires a popular vote and the approval of the miners to implement any improvements to the protocol (Tomaino, 2017). This means all the stakeholders involved must reach a decision via consensus, which instils trust in Bitcoin, but also affects the adaptability of the protocol and limits users' choices in deciding. In case no consensus is reached among the network, the blockchain splits to formulate a hybrid product. For instance, at the moment there are three types of Bitcoin: XT, Classic, and Unlimited. It is important to note that multi-stakeholder decision-making processes are slow and inefficient by nature; when an outcome is achieved, however, implementation is inclusive and democratised. Bitcoin's governance structure might be coded, however, the implementers must have good intentions to execute the mission of a protocol watchdog with honesty.

Understanding Bitcoin's governance structure is crucial to its mainstream adoption because there is no precedented successful moveable asset (money, property, etc.) that does not require vetting from a centralised authority. When an asset is software based, many fail to see how it can be associated with a real value. Not everyone fully grasps why one Bitcoin rallied towards the end of 2017 to reach an unprecedented value of $20,000,[33] and little analysis is available to explain why an unregulated asset's value is unstoppable and beating all speculations. According to Nobel Laureate and former chief economist of the World Bank, Joseph Stiglitz, "Bitcoin is successful only because of its potential for circumvention [and] lack of oversight."[34] Financial experts like him are adamant that Bitcoin must be banned because it is uncontrollable. Developers, however, believe that Bitcoin is already regulated by mathematics, and they take issue with how the concept of governance is associated with "the belief that the technology is broken and needs to be fixed, or that the process has stopped working and needs to be saved. [Bitcoin developers] prefer the word 'stewardship" (Tapscott and Tapscott, 2017).

The Ethereum governance structure is similar to Bitcoin's since it uses PoW mining to reach consensus and a multi-stakeholder structure that involves the miners and the users. The social contract between these stakeholders can thus be understood as the underlying model for the

[33] https://www.coindesk.com/price/.
[34] https://www.coindesk.com/bitcoin-outlawed-economist-joseph-stiglitz-says/amp/.

governance of blockchain-based interactions. The difference between the Bitcoin and Ethereum governance structures, however, resides in the fact that the latter is championed by Vitalik Buterin, the lead developer and the inventor of Ethereum, who happen to be an influential leader who "the community looks to on important protocol and economic decisions" (Tomaino, 2017), unlike Satoshi who is a "silent" leader. Buterin was at the forefront of the Ethereum hard fork event to reverse the DAO hack by organising a democratic vote. The majority agreed to execute the change, and opted in to stay on the chain led by Buterin and the Ethereum Foundation.

This specific governance model illustrates how blockchain technologies are technologically distributed by design, and where participants have a role in the decision-making. Yet, in the event of a critical decision that requires human intervention, the masses always aspire to be led. It is psychologically reassuring for the community to have a leader who can provide guidance, especially in the absence of any enforceable agreements. This is a critical point to the governance of Ethereum because there is a high-risk factor relying entirely on a sound judgment of one person. Even though the majority of Ethereum core developers generally stand behind Buterin, there are rising critical voices warning about its vulnerabilities.

From a legal perspective, there is a need to explore how public and/or private law can provide guide points for blockchain governance. For instance, Patrick Murck, a general council specialised in Blockchain, stressed:

> "Blockchain is truly an innovative approach to governance for networks and machines. But we must resist the temptation to anthropomorphize code and misapply machine governance to social systems. Code is law for machines, law is code for people. When we mix up these concepts, we wind up with situations like the DAO" (Murck, 2017).

From legal and regulatory standpoints, the credibility of blockchain technologies depends on their governance structure. The scope of legitimate practices for blockchain-based systems is fundamentally a governance question, not a computer science one. Yet, current legal systems are challenged by this technology because it pretends to offer enticing solutions when the law does not. It will be important to define synergies between the two to map their respective roles and how they can complement each other or adapt to recognize the potential of the blockchain.

A more progressive theory to blockchain governance suggests that governments and regulators alone lack the expertise to govern this technology. Tapscott and Tapscott, the authors of a 2017

WEF report on the potential of blockchain and one of bestselling books on the topic, *Blockchain Revolution*, quoted Joichi Ito, the director of the Massachusetts Institute of Technology (MIT) Lab, as stating, "You can regulate networks, you can regulate operations, but you can't regulate software" (Tapscott and Tapscott, 2016b). Later, the authors wrote:

> "The genius of distributed ledgers is that the technology must be distributed. Power is distributed. Heavy-handed government intervention would kill this embryonic technology in its egg. Rather, we need self-organizing, bottom-up, and multi-stakeholder governance. In fact, this type of governance is the best protection from government interference and subjugation" (Tapscott and Tapscott, 2017).

The governance structure of blockchain technologies certainly requires further examination, but there could be no specific model to adhere to as a baseline following the examples from Bitcoin and Ethereum; each application governance model is distinct even though they both use the same underlying technology. Part of the governance discussion in public blockchains is their transparency. The next section sheds light on how transparent decentralised consensus and decision-making on these blockchains is.

3.1.1 Decision-making process transparency and decentralized consensus on blockchains

Blockchain governance triggers a debate around the process in place to achieve decentralised consensus. The fact that this technology uses an algorithm to enforce agreements on the global scale increases the risk of the inability to define liabilities. In order to trust blockchains, the general public as well as regulators require guarantees that no specific stakeholder or entity controls them. In practical terms, this is very challenging to prove. Nevertheless, the significant increase of blockchain's concept adoption, along with the increased awareness, education, and media coverage it is garnering, could indicate a slight improvement of the public's perception.

In the case of Bitcoin, power is distributed among all the relevant stakeholders. The rule is that no stakeholder should have more influence or power than any other to change the terms of the Bitcoin protocol. All the parties involved depend on each other to protect network rules, and any change will require coordination and consensus. "So, when Bitcoin software developers began debating about how to increase network capacity, the discussion evolved into a multi-stakeholder melee dubbed a 'governance crisis' by mainstream media" (Murck, 2017).[35] Any change that will affect the core of the Bitcoin protocol is usually faced with resistance. The conservative approach provides more security because it is not possible to circumvent one of

[35] https://techcrunch.com/2015/08/22/money-and-politics-bitcoins-governance-crisis

the three stakeholders to introduce any changes, especially developers, but it also means that such practices can stall collaboration and hinder the improvement of the technology.

The increase in blockchain adoption means reaching consensus regarding changing the rules will be challenging. If the community decides to stick to the original principles of the blockchain, there is a little chance that these networks will submit to traditional governance structures because the essence of blockchain technologies dictate that all participants govern them. "The open-source nature of the Bitcoin protocol makes it technically easy to do. The very objective of consensus algorithms is to distribute the authority to decide the state of the blockchain to a decentralized set of users." (Tapscott and Tapscott, 2016) According to Buterin, there are three different types of decentralized users that correspond to a set of consensus algorithms: "Owners of computing power with standard proof-of-work algorithms; stakeholders with various proof-of-stake algorithms in wallet software; and members of a social network, with a federated-style consensus algorithm. Note that only one of those consensus mechanisms includes the word 'power'" (Tapscott and Tapscott, 2016). This is a hint that the lion's share of decision-making could possibly lie within the miners, who actually have the capacity to power the network, but it does not exclude the importance of other stakeholders since their part is critical to verifying the authenticity of transactions.

The role of miners in particular has increasingly been magnified throughout the blockchain governance debate. For example, there is a perception that miners control the rules of the Bitcoin protocol because of a misunderstanding of the meaning of "miner signalling," as chartered in Bitcoin Improvement Proposal (BIP) 9,[36] where the emphasis was to ensure the uptake among the miner community for any modification must be significant, except that this fact will have no impact on consensus rules as stated in the proposal. "The idea is that miners will signal their readiness for a protocol upgrade before it activates in an attempt to make sure the deployment goes smoothly" (Torpey, 2017). The users execute these updates as well before miner signalling occurs, which gave the impression that miners have a say in any Bitcoin protocol additions. Blockstream CEO Adam Back explained to Forbes that "there were a lot of people who genuinely believed that miners decided on the protocol [rules], where it's actually a complete misunderstanding because it's the economic nodes – so anybody who runs a full node (a computer that has a complete copy of the blockchain, and is able to verify all the transactions since the start) for their own verification (any business, any investor, whatever) –

[36] https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki.

100,000 nodes on the network, that's what defines the consensus rules" (Torpey, 2017). Therefore, miners' role beyond mining activities, which includes creating blocks as quickly as possible to be rewarded, revolves around "providing a security service to whichever chain they want to provide a security service to, and the users and investors are creating the value for the supply and demand of the coin," according to Back. "Miners just follow that. They follow the profit" (Torpey, 2017).

The misinterpretation of blockchain stakeholder's roles – specifically the miners, developers and other users – the politicisation of consensus rules, and the continuous alterations to the core protocols, however, trigger crucial questions on how to achieve mainstream adoption of this technology without compromising on its core principles. Understanding the distributed and decentralised consensus might be a given in expert circles, but still ambiguous to the public and can lead to the wrong outcome in terms of asserting the transparency of decisions on a blockchain.

Immutable consensus on blockchain reinforces the notion of accountability as well. Nevertheless, public blockchains are political because of the way they allow a majority elected transaction to sit on a block. It is still up to the network to validate and approve it, which leaves enough space for unpredictable dynamics among the network in decision-making. Therefore, the transparency of decisions on a blockchain can be associated with the specific interest of the participating users. The next paragraph will elaborate further on the issue of soft power accumulation in distributed structures and to what extent it influences the decision-making process on a blockchain.

3.2 Soft Power accumulation in distributed structures

The notion of distributed power among the blockchain nodes mitigates the risk of greater influence of a specific stakeholder at the expense of another. All nodes are treated equally as participants, they all adhere to the same network rules, and they all need to give approval for any changes to the core protocol. The equal-footing treatment of participating nodes does not exclude the possibility that these nodes could eventually self-organise in smaller groups, or as a coalition that has a common interest to build consensus over a specific event on the blockchain or to defend their own interest(s).

As previously stated, the growing number of blockchain participants makes it difficult to reach consensus on any changes, which makes the newcomers more akin to followers, and inadvertently allows the core developers – i.e., "the code protectors" – to become gatekeepers. The intentions of the code's core developers resisting change might be to genuinely maintain the integrity of the blockchain. Yet, it also raises the crucial question of whether or not blockchain technologies are truly governed by everyone who participates in them simply because two board, informal categories of participants have emerged: the gatekeepers who seem to hold the key to the door, and the gate watchers who seem to play a role of a "witness" to solely validate information entry, but do not really contribute to key decisions regarding the specific blockchain application. Nevertheless, the gate watchers do play a key role in building trust in and scaling up the network, which allows a blockchain to create new business opportunities where they could not exist before due to myriad political and/or economic reasons.

Algorithmic transparency and consensus-based trust in blockchains could form a key element of its good governance, but soft power accumulation within the nodes can shift the balance of decision-making power. This is because the participants' motivation could solely be materialistic and not necessarily specific to building trust in the blockchain, nor is it dedicated to validating its current governance structure.

This can be illustrated in the fact that most Bitcoin miners and exchanges are based in China, and here the reference does not point to the role of miners in influencing protocol rules because it was previously established in this dissertation that this assumption is not correct. Early investors in Bitcoin mining from China seized the opportunity to build mining farms with custom-made computational power as a business venture. This was significantly boosted by

the low cost of energy, and the availability of financial resources to invest in the required infrastructure and hardware to mine Bitcoin as a pure investment opportunity, which comes with a huge risk of price fluctuation and uncertainty. These thoughts materialised towards the end of 2017 when the price of Bitcoin was considerably volatile, but ultimately crashed due to the speculative nature of trading in the financial markets.

The high risks of this business pushed away competition for some time to allow Chinese companies to thrive in the field of Bitcoin mining, including chip manufacturers, who invested the time and money in fully customized design chips and graphics cards, but these early investors cannot always afford to bet on the future success of Bitcoin (Peck, 2017). The realisation of China's dominance in mining cryptocurrencies and the exchanges business raised even more questions among industry watchers, and certainly prompted deeper consideration of the power dynamics within cryptocurrency communities. [37]

Until today, there is no reason to suggest that China's mining companies and exchanges have a hidden agenda to use their accumulated soft power to influence how Bitcoin is governed. If it is the case, do we have to worry about it? What about the motives of miners and exchanges in other jurisdictions who also have a share in the market? Just like in the Internet governance filed, it is very challenging to define these miners' agenda when the whole industry works in silos, yet is it clear that these entities are certainly driven by profit until a decision like banning Bitcoin exchangers in China all together rings alarming signals about the future of cryptocurrency.

In September 2017, China banned Bitcoin exchanges from operating because of the lack of a regulatory framework to organise trading cryptocurrencies on these platforms, which would also affect miners. It is a very recent development and there is a fair amount of analysis why China would make this move, but a logical prediction is that the Chinese government has the ambition to create its own China-centric cryptocurrency for its own niche market. China has a unique business strategy where it either invests in obscure markets like many in Africa, or bans technology products to create its own. Beyond the censorship narrative, there is a logical financial reason for China to domesticate technology products: the significant market share it represents. It is profit that drives these decisions.

[37] A list of top mining companies is available at: http://uk.businessinsider.com/bitcoin-pools-miners-ranked-2015-7/#21-unknown-entity--01-1.

Soft power accumulation in distributed structures in general but specifically in blockchain requires further analysis to establish if it hinders their good governance. The financial motivation of miners lands them the important role of building and maintaining trust in the chain, but it also triggers questions around how to create a balance between their interest and power of influence as a majority when it comes to validating blocks. The need of miners is counterbalanced by the energy required to conduct the PoW, and that is why Ethereum is currently exploring the option to switch from the PoW consensus model to the proof of stake (PoS) consensus mechanism "where miners become validators and needn't to spend energy to vote" (Tapscott and Tapscott, 2017), but it also means they will not get the same large rewards.

Using this method of securing consensus affects miners' incentives to participate in the governance of the blockchain. According to Tapscott and Tapscott (2016), the shift from PoW to PoS:

> "Adds a dimension to innovation: not only must developers worry about whether their new features and functions will work in their own right, but they must also check how the choice of consensus algorithm keeps them secure and distributed to the most appropriate economic set. Where 51 per cent of hacking attacks on proof-of-work models stem from concentrated mining power: a group of miners controlling more than 50 per cent of the network's computing power can sabotage transaction verification; attacks on proof-of-stake models come from concentrated coin control, and coin exchanges are typically the biggest stakeholders"

This means that exchanges could have a significant impact on the economic implementation of blockchains, and potentially morph into a key stakeholder in a blockchain's technical deployment. In other words, imagine the consequences if a trading platform on over-the-counter markets suddenly became a decision-maker on the value of the traded products

Experimenting with various algorithmic adjustments to address some of the features of blockchain technologies certainly provides a platform to test the boundaries of this technology, which seems to thrive on peer-to-peer collaboration as intended. There is a little indication if the network will embrace these adjustments, however. If the majority refuses the adjustments, not only does it affect the distributed consensus governance model, it also makes the concept of entrusting an algorithm – i.e., a code to govern the "society" – questionable. The majority concept is central to blockchain discussions, but what about the rights of the network's minority? The last section of this dissertation addresses initial ideas on how to maintain minority interest in majority-base consensus systems and how it relates to the governance structure of blockchain technologies.

3.2.1 Safeguarding minority interest in majority-based consensus systems

Blockchain technologies derive their legitimacy from a majority-based, distributed consensus model, which poses a governance challenge regarding how to maintain incentivising the network for mass collaboration. On the other hand, it raises the question of how a majority-based consensus system can adequately protect the rights of the minority, specifically where voting influence is weighted proportionally vis-à-vis the number of tokens held.

In order to grasp the concept of majority rule, it is worth exploring the idea within a political system. This principle has several functions, including the establishment of a clear mechanism for making decisions, and where a majority of 50 per cent plus one decides an issue or question. This ensures that the decisions made are agreed upon by the majority than the opposite (Democracy Web, n.d.). The principle of majority rule here is vital to ensure that decisions are enforceable and that minorities could not stop the majority from taking decisions.

The majority consensus rule on a blockchain is incentivised by economic gain and not by democracy. In the case of Bitcoin, the protocol maintains significant economic incentives to sustain hardcore miner decentralisation. Therefore, any adjustments to the original Bitcoin protocol should take into account the high value of the network's miners because of the key role they play in verifying transactions and confirming blocks in exchange for Bitcoins (Tapscott and Tapscott, 2017).

According to Bitcoin core developer Peter Todd, "The economic incentive principle benefits even smaller miners in geographically dispersed locations and should allow them to compete with larger miners in geographically centralised locations like China." This statement raises an important question on how to incentivise such miners when Bitcoin rewards is zeroed after the pre-set ceiling of 21 million Bitcoins is hit It seems clear, though, that there will always be a disparity between these two segments in terms of the profit generated because their mining capabilities are not equal – especially when the market price of Bitcoin hits a higher price.

Nevertheless, small miners aspire to increasing their odds to get part of the spoils by pooling their computing power with the nodes. When the total number of coins is exhausted, Nakamoto (2008) proposed a solution to apply a fee structure per transaction to incentivise the nodes and to compensate them for verifying the transactions. He also Anticipated power play between the

nodes, which can undermine the integrity of the network if miners focus only on their profit. Nakamoto (2008) explained how:

> "The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth."

Such principle can eventually mean that a single miner stands the chance to be equally treated as a minority if he/she plays by the rules.

Applying transaction fees to incentivize miners is also important to safeguard the network's stability. The block reward motivating the miners keeps halving because each time a new valid block is added to the Bitcoin network, the reward is half of what it used to be. Initially, the reward was set to 50 Bitcoin, but it then fell to 25, and is expected to hit 6.25 by 2020.[38] As a result, the hash rate, the speed in which a node competes to solve complex mathematical computations to find a block, will automatically drop. This will trigger a network vulnerability leading to the 51 per cent attack, where a huge mining pool or a cartel of large mining pools controls 51 per cent of the hash rate (Tapscott and Tapscott, 2017). In such situation, a majority vote of miners could hijack block generation to compose their version of the truth on the Bitcoin network. While they will not be able to make any money, they could reverse their own transactions within a previous block to get their purchase back. "It would mean going back and redoing the block that contained all their purchases as well as all subsequent blocks, even as the network continues to generate new blocks. When the cartel's branch became longer, it would become the new valid one" (Tapscott and Tapscott, 2017). Nakamoto (2008) theorized, however, that such move would be prohibitively expensive, even more so than mining new coins, and miners would not opt in for it. The on-going probability of splitting the blockchain by majority miners weakens the principle of decentralised consensus, though, and brings the fairness of the process into question vis-à-vis the rights of minorities on the network and its resilience capability to fend off majority attacks.

There are still many questions regarding how to link blockchain's core principles to how it is governed, but there are little convincing answers that offer a clear picture to the common

[38] This webpage specifies all the information about the current number of mined Bitcoins, and provides a timeline to showcase all the details, including prices, percentages, values, etc. See: http://www.bitcoinblockhalf.com/.

reader. It is unlikely that code governance discussions appeal to the potential stakeholders due to its complexity, but also because we are in the early stages of testing the concept as a whole.

This indicates that future research should focus on investigating blockchain governance beyond the code, transparency of decisions, or consensus rules. There is an important aspect that is yet to be explored relating to the governance question, namely identifying blockchain design parameters for robust governance structures that incorporate and align with the interests of stakeholders, and are flexible enough to withstand future vulnerabilities. It is also crucial to identify a set of decentralized communication and information tools that enable decentralized consensus, support transparency in the decision-making process, and do not produce or empower hidden gatekeepers.

Governance in the context of blockchain technologies is divided between the arrangements that regulate nodes participating in the network and the baseline of consensus rules. Permissioned blockchains are more likely to be governed by specific contracts giving leverage to the entity or business that deployed the blockchain to be in full control to choose their preferred governance structure. Yet, there is no clear understanding within the blockchain industry as to what governance in the context of blockchain technologies should look like. In the case of permissionless systems, the concept of coding governance has its own limitations as discussed previously, and will require proofing to ensure that the whole concept lives up to the expectations of blockchain technologies removing the role of centralised forms of governance.

Blockchain technologies promise to alter society's perception about how we exchange values over the Internet and whom we trust. In this vein, the governance question needs to take a central stage in future discussions because defining the answers will help provide validation of the concept, as well as set the scene to the shift towards decentralised structures in not only systems, but also states, establishments, and organisations. Blockchain technologies could hold the important value of democratising the world and shift the balance of power from a handful of people to the masses; then again, it could also just be a hyped-up technology that will eventually go the way of Betamax or Internet Protocol version 4 (IPv4), or another manifestation of inequality judging by how Bitcoin, the first implementer of blockchain technology, has been elitist by excellence.

Nevertheless, it is crucial to recall the valid reasons behind the concept of blockchain takeover, which could be simply summarised in the persistent crisis of legitimacy of our institutions and the decline of trust and value of our exchange media. It will take significant work to restore

trust in social and governance systems, and to maintain the transparency and accountability of both public and private institutions. Equally important, however, is for blockchain developers to demonstrate how the technology works beyond the proof of concept. Given current limited progress, building solid market share embedded with long-term vision is elusive at best. Most investments in the technology are speculative and aim at quick wins.

Conclusion

Necessity is the mother of invention, and blockchain technologies aspire to address issues triggered by the role of intermediaries in any medium where data, information, money, property, or value is exchanged. There is a crisis of trust in public and private institutions and centralised mechanisms of decision-making; thus, if blockchain is to deliver on its promise to cut out the middleman, it will constitute a huge leap towards instilling the principles of transparency, trust, and accountability – the key criteria of any exchange operation.

Blockchain technologies' combination of core features offers a unique solution to build trust in a transaction based on a unanimous, algorithmic consensus mechanism that allows market participants to be key stakeholders in the decision-making process. This set up suggests that the development process of blockchain technologies genuinely attempts to overcome the trust crisis by addressing all the weak points of a traditional medium of exchange. Nevertheless, this research identifies how some of blockchain's core features can be challenged in practice. The transparency of the ledger occurs at the expense of the notion of privacy, and if not addressed adequately, it will almost certainly dissuade the financial industry, which is keen on maintaining the confidentiality of assets it handles, from participating.

Other features such as security and the immutability of blockchain technologies are questioned due hacking events that took place in two of the most widely known and widely used blockchain applications. I established that a compromise between some the principles might be required in order to maintain the integrity of blockchain technologies as a whole. Moreover, given that blockchain adoption is still in the experimental stage, it is important to understand its vulnerabilities in the specific context of incidents when they occur and not holistically.

Decentralized blockchains will balance out centralized authority with their strong consensus, and privacy-protecting focus, which will provide a powerful set of checks and balances on the excesses of centralized systems. It occurs in this specific circumstance that the buy-in to the technology behind the concept is much more important than trust because the latter is inherently guaranteed by design in a blockchain.

The decision-making on a blockchain occurs at the application level, which normally does not include or require a regulatory framework or any kind of interference from a third party. The traditional scenario in all newly launched technologies is that every innovation has ample room

to benefit from some level of autonomy until regulation catches up with it. The second chapter of this dissertation covered the role of regulation in deploying blockchain, the policy and legal implications of this technology, and how such regulation affects service delivery and economic relationships powered by blockchain technologies.

Regulation provides safeguards to investors and consumers, but it can also stifle innovation. The current approach to blockchain technologies varies as some countries are introducing specific regulatory and policy frameworks to promote innovation and growth, while preventing systemic risk, ensuring financial stability, and protecting consumers and entrepreneurs against economic harm and illegal activity.

The current regulatory trend of blockchain-powered products suggests that governments' approach is slow and cautious in Europe, and radical in Asia. The US is not reinventing the wheel and taking steady steps to classify blockchain powered digital currencies within the existing categories of financial products.

In order for blockchain technologies to be disruptive, they need to foster creative solutions to key industries and catalyse economic transformation. This starts with addressing the policy challenges that can potentially impact its adoption. It was established that ensuring privacy by design on private blockchain applications is doable by applying new techniques, which makes privacy an inherent feature on a blockchain. On the other hand, there is no one-size-fits-all solution to address the security question because it will all depend on which type of blockchain is adopted. Large companies are likely to opt in for private blockchains where the stability and efficacy of the platform are guaranteed.

The ethos of blockchain technologies is practically agnostic to existing legal and regulatory frameworks because the entire concept revolves around building a reputation in a trustless environment that completely avoids the judgment of a centralised authority. Scaling the concept and applying it to business operations, however, shifts our attention to protection mechanisms to safeguard property rights when things go wrong. Hence, the focus on the legal identity of blockchain participants is of utmost importance to define liabilities.

There is a need to define the intersection between legal and technical code to shape regulatory frameworks by combining both to ensure blockchain technologies comply with legal rules. Smart contracts pose new complications that are not only challenging to existing regulatory

frameworks, but also to the concept of regulation itself. Blockchain technologies challenge the status quo stipulating the rules and aims to restore decision-making power back to the masses.

On the issue of blockchain technologies' governance structure, permissionless blockchains will not survive without having a credible governance mechanism. The scope of legitimate practices for blockchain-based systems will require a well-defined checks and balance mechanism in plain simple language. Immutable decentralised consensus on a blockchain reinforces the notion of accountability. Nevertheless, blockchain technologies allow a majority-elected transaction to sit on a block. It is still up to the network to validate and approve it, which leaves enough space for unpredictable dynamics among the network in terms of decision-making. Therefore, the transparency of decisions on blockchains can be associated with the specific interest of the participating users.

Algorithmic transparency and consensus-based trust in blockchain technologies could form a key element of its good governance, but it is observed that that soft power accumulation within the nodes can shift the balance of decision power since the motivation of participants could be solely materialistic and not necessarily specific to building trust in the blockchain, nor is it dedicated to validating its current governance structure. Soft power accumulation in distributed structures and specifically in a blockchain requires further analysis to establish if it hinders their good governance.

Finally, the majority concept is central to blockchain discussions; however, the rights of the network's minority prove to be equally important otherwise blockchain technologies risk becoming another manifestation of a centralised authority. The principle of majority rule is vital to ensure that decisions are enforceable and that minorities could not stop the majority from taking decisions. The majority consensus rule on a blockchain is incentivised by economic gain and not by democracy.

Bibliography

Acheson N (2017a) Blockchain Regulation: Is Europe Getting It Right? *CoinDesk*, 15 May. Available at https://www.coindesk.com/blockchain-regulation-europe-getting-right/ [accessed 13 November 2017].

Acheson N (2017b) China's ICO Ban: Understandable, Reasonable and (Probably) Temporary. *CoinDesk*, 12 September. Available at https://www.coindesk.com/chinas-ico-ban-understandable-reasonable-probably-temporary/ [accessed 13 November 2017].

Adams M (2016) *Blockchain: The History, Mechanics, Technical Implementation And Powerful Uses of Blockchain Technology*. CreateSpace Independent Publishing Platform, p.20

Akhtar T (2017) SEC Weighs In on ICO Tokens as Securities; Ether Still Labeled "Currency." *Bitcoin Magazine*, Available at https://bitcoinmagazine.com/articles/sec-weighs-ico-tokens-securities-ether-still-labeled-currency/ [accessed 13 November 2017].

Andreev O (2017) Hidden in Plain Sight: Transacting Privately on a Blockchain. *Chain*, Available at https://blog.chain.com/hidden-in-plain-sight-transacting-privately-on-a-blockchain-835ab75c01cb [accessed 6 October 2017].

Andress J (2014) *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Syngress, p.31

Asharaf A and Adarsh A (2017) *Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities: Emerging Research and Opportunities*. IGI Global, p.50

Bashir I (2017) *Mastering Blockchain*. Packt Publishing Ltd, pp. 17-57

Bear K (2017) How will regulation impact the development of blockchain technology ? *Finextra Research*, 6 May. Available at https://www.finextra.com/blogposting/14054/how-will-regulation-impact-the-development-of-blockchain-technology- [accessed 18 October 2017].

Berke A (2017) How Safe Are Blockchains? It Depends. *Harvard Business Review*, 7 March. Available at https://hbr.org/2017/03/how-safe-are-blockchains-it-depends [accessed 6 November 2017].

Bitlegal (2017) *Abu Dhabi's stance on ICOs | BitLegal*. Available at http://bitlegal.io/2017/10/11/abu-dhabis-stance-on-icos/ [accessed 13 November 2017].

Blockstream (2017) Different Approaches to Privacy on the Blockchain. Available at https://blockstream.com/2017/09/08/different-approaches-to-privacy.html [accessed 26 October 2017].

Breitman K (2017) Op Ed: Why Ethereum's Hard Fork Will Cause Problems in the Coming Year. *Bitcoin Magazine*, Available at https://bitcoinmagazine.com/articles/op-ed-why-ethereums-hard-fork-will-cause-problems-coming-year/ [accessed 15 November 2017].

Buterin V (2016) *Privacy on the Blockchain*. *Ethereum Blog*. Available at https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/ [accessed 25 October 2017].

Buterin V (2017) *The Meaning of Decentralization*. *Vitalik Buterin*. Available at https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 [accessed 9 October 2017].

CFA (ICFAI) PB (2014) Blockchain. *Investopedia*, 13 June. Available at http://www.investopedia.com/terms/b/blockchain.asp [accessed 22 September 2017].

Chen A (2016) We Need to Know Who Satoshi Nakamoto Is. *The New Yorker*, 9 May. Available at https://www.newyorker.com/business/currency/we-need-to-know-who-satoshi-nakamoto-is [accessed 25 September 2017].

Das S (2017) Australia's Bitcoin Regulation Bill Gets the Green Light. *CryptoCoinsNews*, 16 October. Available at https://www.cryptocoinsnews.com/australias-bitcoin-regulation-bill-gets-green-light/ [accessed 18 October 2017].

Democracy Web (No date) Majority Rule/Minority Rights: Essential Principles | Democracy Web. Available at http://democracyweb.org/majority-rule-principles [accessed 9 January 2018].

Drescher D (2017) *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Apress ,p.37

DTCC (2017) Blockchain & Distributed Ledgers: 8 Features Explained. Available at http://www.dtcc.com/news/2016/february/17/eight-key-features-of-blockchain-and-distributed-ledgers-explained [accessed 2 October 2017].

EBA (2014) *EBA Opinion on 'virtual currencies.'* Available at http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf [accessed 18 October 2017].

Ethereum Project (2017) Ethereum Project. Available at https://www.ethereum.org/ [accessed 10 November 2017].

Gabission G (2017) Policy Considerations for the Blockchain Technology Public and Private Applications - EU Science Hub - European Commission. *EU Science Hub*, 6 April. Available at https://ec.europa.eu/jrc/en/publication/policy-considerations-blockchain-technology-public-and-private-applications [accessed 15 November 2017].

Goenka H (2018) Bitcoin Mining Cost Lowest In Venezuela, Highest In South Korea, Report Finds. *International Business Times*, 27 January. Available at http://www.ibtimes.com/bitcoin-mining-cost-lowest-venezuela-highest-south-korea-report-finds-2646191 [accessed 31 January 2018].

Groopman J (2017) *Four Examples of Blockchain-Artificial Intelligence Deployments | Tractica*. Available at https://www.tractica.com/artificial-intelligence/four-examples-of-blockchain-artificial-intelligence-deployments/ [accessed 31 January 2018].

Haring B (2017) *Blocktribune. NSA Has Identified Satoshi Nakamoto*. Available at http://blocktribune.com/nsa-identified-satoshi-nakamoto-author-claims/ [accessed 25 September 2017].

Hofmann E et al. (2017) *Supply Chain Finance and Blockchain Technology: The Case of Reverse Securitisation*. Springer, p.56

Jia C (2016) Op-Ed: What Is the True Meaning of "Decentralization" in Blockchain Technology? *Bitcoin Magazine*, Available at https://bitcoinmagazine.com/articles/guest-post-what-is-the-true-meaning-of-decentralization-in-blockchain-technology-1474558340/ [accessed 9 October 2017].

Karame GO and Androulaki E (2016) *Bitcoin and Blockchain Security*. Artech House,p.48

Kurbalija DJ (2016) *An Introduction to Internet Governance: 7th edition*. Diplo Foundation, p.21

Laurence T (2017) *Blockchain For Dummies*. John Wiley & Sons, p.25

Lessig L (2006) *Code: And Other Laws of Cyberspace, Version 2.0*, 2nd Revised ed. edition. New York: Basic Books, p.77

McKinlay J et al. (2017) Blockchain: background, challenges and legal issues | Insights | DLA Piper Global Law Firm. *DLA Piper*, Available at https://www.dlapiper.com/en/germany/insights/publications/2017/06/blockchain-background-challenges-legal-issues/ [accessed 8 November 2017].

Mougayar W (2016) *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. John Wiley & Sons, p.61

Murck P (2017) Who Controls the Blockchain? *Harvard Business Review*, 19 April. Available at https://hbr.org/2017/04/who-controls-the-blockchain [accessed 30 November 2017].

Nakamoto S (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Available at https://bitcoin.org/en/bitcoin-paper [accessed 1 February 2018].

NASDAQ (2017) What Is an ICO? *NASDAQ.com*, 10 August. Available at http://www.nasdaq.com/article/what-is-an-ico-cm830484 [accessed 11 November 2017].

NortonRoseFulbright (2016) Unlocking the blockchain: A global legal and regulatory guide - Chapter 1. Available at http://www.nortonrosefulbright.com/knowledge/publications/141573/unlocking-the-blockchain-a-global-legal-and-regulatory-guide-chapter-1 [accessed 8 November 2017].

Parker Q (2016) Ethereum Blockchain Hack Reversed. Available at http://techportfolio.net/2016/07/blockchain-hack-reversed-while-banks-look-on/ [accessed 7 October 2017].

Peck ME (2017) Why the Biggest Bitcoin Mines Are in China. *IEEE Spectrum: Technology, Engineering, and Science News*, 4 October. Available at

https://spectrum.ieee.org/computing/networks/why-the-biggest-bitcoin-mines-are-in-china [accessed 8 January 2018].

Qureshi H (2017) A hacker stole $31M of Ether — how it happened, and what it means for Ethereum. *freeCodeCamp*, 20 July. Available at https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce [accessed 7 October 2017].

Redman J (2018) *These Dutch Researchers Are Mining Cryptocurrencies With Body Heat*. *Bitcoin News*. Available at https://news.bitcoin.com/these-dutch-researchers-are-mining-cryptocurrencies-with-body-heat/ [accessed 31 January 2018].

Rees T (2017) Regulating Bitcoin: how new frameworks could be a catalyst for cryptocurrencies. *The Telegraph*, 16 April. Available at http://www.telegraph.co.uk/business/2017/04/16/regulating-bitcoin-new-frameworks-could-catalyst-cryptocurrencies/ [accessed 18 October 2017].

Richards JP Tim O'Donnell, and Kimberly (2016) A Strategist's Guide to Blockchain. *strategy+business*, Available at https://www.strategy-business.com/article/A-Strategists-Guide-to-Blockchain?gko=0d586 [accessed 2 October 2017].

Rome Z (2017) Securing Blockchains with Hardened Encryption. *Futurex*, Available at https://www.futurex.com/blog/securing-blockchains-with-hardened-encryption/ [accessed 6 November 2017].

Smolenski N (2017) *The EU General Data Protection Regulation and the Blockchain*. *Medium*. Available at https://medium.com/learning-machine-blog/the-eu-general-data-protection-regulation-and-the-blockchain-1f1d20d24951 [accessed 30 October 2017].

Tapscott D and Tapscott A (2016) *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York: Portfolio, p.6

Tapscott D and Tapscott A (2016)(b) *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World*. Penguin UK, p.23-40

Tapscott D and Tapscott A (2017) Realizing the Potential of Blockchain. *Blockchain Company*, Available at http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf [accessed 27 November 2017].

Tennison J (2016) What is the impact of blockchains on privacy? | News. *Open Data Institute*, Available at http://theodi.org/blog/impact-of-blockchains-on-privacy [accessed 15 November 2017].

Terekhova M (2017) More Bitcoin regulations are coming. *Business Insider*, Available at http://uk.businessinsider.com/more-bitcoin-regulations-are-coming-2017-7 [accessed 18 October 2017].

The Economist (2017) Regulators begin to tackle the craze for initial coin offerings. *The Economist*, Available at http://www.economist.com/news/finance-and-economics/21731157-they-raise-difficult-legal-questions-regulators-begin-tackle-craze [accessed 10 November 2017].

The Elements Project (No Date) Confidential Transactions. Available at https://elementsproject.org/elements/confidential-transactions/ [accessed 6 November 2017].

Tomaino N (2017) The Governance of Blockchains. *The Control*, 28 February. Available at https://thecontrol.co/the-governance-of-blockchains-5ba17a4f5da6 [accessed 27 November 2017].

Torpey K (2017) 2017 Was The Year When Everyone (Finally) Learned Bitcoin Isn't Controlled By Miners. *Forbes*, Available at https://www.forbes.com/sites/ktorpey/2017/11/30/2017-was-the-year-when-everyone-finally-learned-bitcoin-isnt-controlled-by-miners/ [accessed 9 December 2017].

Wang K (2017) Governance in Blockchain Part I: The Bitcoin Experiment. *ITNEXT*, 8 August. Available at https://itnext.io/governance-in-blockchain-part-i-the-bitcoin-experiment-a8c633791e6d [accessed 24 November 2017].

Meleo A What is Blockchain Technology? Crypto & Blockchain Explained - Business Insider. no date. Available at http://uk.businessinsider.com/blockchain-technology-cryptocurrency-explained-2017-8 [accessed 21 September 2017].

Williams-Grut O (2016) The technology behind bitcoin could solve a big problem banks had in the 2008 crisis. *Business Insider*, Available at http://uk.businessinsider.com/itbit-ceo-blockchain-2008-financial-crash-risk-settlement-2016-2 [accessed 25 September 2017].

Young J (2017) Bitcoin and Ethereum Price Recover From Korea ICO Ban as Japan Licenses Exchanges. *CryptoCoinsNews*, 29 September. Available at https://www.cryptocoinsnews.com/bitcoin-ethereum-price-recover-korea-ico-ban-japan-licenses-exchanges/ [accessed 18 October 2017].