“The authority of the steam”: power dynamics of digital production in the Bitcoin blockchain

by

Pablo Rodrigo Velasco González

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Interdisciplinary Studies

University of Warwick

Centre for Interdisciplinary Methodologies

September 2017

Table of Contents

Figures

Acknowledgements

This work would have not been possible without the guidance of my supervisor, Nathaniel Tkacz. I was very lucky to have his counsel, patience, and helpful close readings (despite my many last-minute submissions). He was an excellent mentor, who helped me sail the unknown waters of pursuing a PhD.

Celia Lury and Michael Dieter (my co-supervisor) were of the greatest help during my time at CIM, I truly appreciate their advice, agile support, and comments on my work. I would also like to thank Christian Ulrik Andersen and Geoff Cox for their comments and feedback on the notions of designed scarcity and superabundance used in Chapter One; and to Sam Hind, who suggested the use of "utopia" as an overarching concept for this work. Richard Terry, Joanna Cuttell, Charlotte Reypens, Tatjana Seitz, and Lisa Stoltz helped me with my writing struggles. By virtue of their suggestions my thoughts were turned into something readable.

A special thanks to *March* (Hanzhi Ruan), *Taz* (Tatjana Seitz), and Maria Punina, with whom I have had numerous long walks and the deepest conversations (both affective and intellectual) throughout this research journey; to my research colleagues: Charlotte Reypens, Loup Cellard, Lisa Stoltz, Nathalie Mezza, Laura Guzmán, and Nadia Jankovicova, who are now my borrowed happy/silly/supportive family; and to the *paraders*: Simone Traini, Ila Bharatan, Danae Arroyos, Christina Meyer, and Yousif Hanna, which are the definition of the best lazy Sunday. I have had many happy days talking and laughing with these people. All were (and still are) the daily sun in an always rainy England.

Thanks to my homes and hosts in Europe, who helped me to present my work outside the Midlands: Mijael and Maria (London), the most heart-warming friends, comrades, and party animals since ever; Tirso, who has managed to be around for a beer, a hug, and a challenging talk for almost two decades now (York); Regina and Jimena, my most cool and loving cousins (Barcelona); Lucho, Rubí and little Emilio (London); Diego "the otamatone" (Delft); Carlos and Vero (Berlin); and Uli *und* Inge, who fed me with the best original German food and stories (Würzburg).

I am grateful to my beloved family, who have given me unconditional love and support since before I was able to speak. Mamá, Papá, Marisol, I love you. I am forever in debt (the good kind) to them. And to my late grandmother, who never understood what I was doing, but was nonetheless always extremely proud and happy for me.

Finally, thanks to Silvia, who inspired me to pursue a PhD (among many more adventures), and supported me greatly during most of the process and in the most obscure times. She shines, uninterruptedly, over a great length of this work.

This thesis was written with the financial support of the Mexican National Council for Science and Technology (CONACYT). Scholarship no. 240176/359291.

Declaration

This thesis is submitted to the University of Warwick in support of my application for the degree of Doctor of Philosophy. It has been composed by myself and has not been in any previous application for any degree. Parts of it have been published by the author as follows:

Modified sections of Chapter One were previously published in:

- Velasco González, Pablo. 2016. 'Superabundant Design: From Waste to Control in Bitcoin Mining'. *A Peer-Reviewed Journal About*, no. Excessive Research (March). http://www.aprja.net/?p=2927.

Modified sections of Chapter two and four were previously published in:

- Velasco González, Pablo. 2016. 'Sketching Bitcoin: Empirical Research of Digital Affordances'. In *Innovative Methods in Media and Communication Research*, by Sebastian Kubitschko and Anne Kaun, 99–122. Palgrave Macmillan.

Summary

This thesis offers a critical investigation of the Bitcoin currency and the operation of its technical structure, i.e. blockchain technology. The main objective of the research is to identify and describe the specific power dynamics performed by and through this digital phenomenon. “Power dynamics” are framed in this work largely in terms of authority and sovereignty.

To structure an exploration of such dynamics, the narrative is overarched by four different notions of “utopia” —as paradox, ideal, no-place, and imagined governance— that address the following main questions always underpinned by the general inquiry on power: What is the Bitcoin Blockchain? Where is it located? How are power relations performed in it? And how are power relations modified in relation with previous institutional systems? The thesis addresses distinct notions of authority in Bitcoin through the observation of its historical, spatial, and organizational characteristics. It maps the techno-political emergence of the blockchain system, the geographical distribution of Bitcoin’s infrastructural network, and the strategies for governance involved in its development as software.

Based on the observation of these settings, this thesis argues that Bitcoin posits a restructuration of power dynamics through the automation of code, in particular, through its process of production. In order to develop this restructuration, the power dynamics of the Bitcoin blockchain are weighted against authority models of the state’s institutions. The thesis builds upon existing political theories of Empire (Hardt and Negri), protocol (Galloway), and the Stack (Bratton) to develop a critical account of Bitcoin’s power dynamics. The work sits in between the disciplines of Media Theory, Software Studies, Political Theory, and Digital Methods, and makes use of qualitative and quantitative methods to empirically support the former argument.

Introduction

At the beginning of 2014 Davi Barker, a self-described anarcho-capitalist and editor of the *dailyanarchist.com*, claimed to be momentarily detained and questioned on his departure from Manchester airport (New Hampshire) (Barker 2014). Barker and his colleague, Bill Buppert (host of *zerogov.com*), were coming back from the New Hampshire Liberty Forum, a convention hosted by the Free State Project, described as "an effort to recruit 20,000 liberty-loving people" ('Free State Project' 2017) and which seeks to limit the role of government to *at most* protect people's rights. Barker was carrying around 100 metal pins, which he was selling at the convention. Having opted-out of the full body scanner, his luggage was meticulously inspected by authorities. At the end of this inspection he was intercepted again, this time by two men who at first refused to identify themselves. The men asked if he was carrying more than $10,000 and planning to travel internationally. On his unwillingness to answer, one of the men —later identified as a Transport Security Administration (TSA) agent— told him: "We saw Bitcoin in your bag and need to check". Bupper, his colleague, replied to the agents: "You can't *see* Bitcoin". After a short, bewildered moment, the agents determined that Barker was not travelling abroad and he was left to his own devices.

This rather odd and seemingly incidental occurrence, nonetheless opens out onto many elements regarding the Bitcoin phenomenon that are central to this study. On closer inspection, Barker's anecdote brings together in a condensed way, some of the most pressing questions surrounding this digital cryptocurrency; questions concerning materiality, ownership, governance, territoriality, and performance. Can bitcoins be physically held? If not, in what form are they owned? How and where are they stored? Can this space be geographically located? Which authority resides over the production, exchange, and transportation of bitcoins? The awkward interaction with the airport's security also signals an unclear situation between the digital object and the TSA as a representative of the US government's authority. Indeed, Barker's main concern in his post about the airport incident is to warn other Bitcoin enthusiasts that the

government (or at least the TSA) *is looking for your bitcoins*. Barker belongs to a diverse group in favour of minimizing state influence. Among this group, Bitcoin is seen as a technical replacement for some of the administrative and regulatory operations of the state. The location of this incident is also significant, as airports often serve as boundaries for the territorial limits of the nation-state authority.

This thesis critically addresses the types of questions that are manifested in this incident of Bitcoins at the border. More specifically, it interrogates how different notions of authority, border, governance, law, space, and regulation are reformulated, or not, by the digital phenomena of the blockchain. I explore this reformulation partly in its relation to the state; not only because of the common association of Bitcoin with libertarian politics (Golumbia 2016), but in particular because the previously listed notions (border, governance, law, regulation, etc.) are structural parts of the state apparatus. My inquiry goes beyond how Bitcoin as a currency relates to government issued "fiat" and is not especially interested in the question of whether or not Bitcoin is a real competitor with state-backed fiat currency. Instead, this research is more concerned with the power dynamics that are reformulated through a technology such as the blockchain, which in the specific case of Bitcoin is commonly framed in terms of its economic qualities.[1] Thus, while I take into consideration the economic relevance of Bitcoin, I observe this quality through a prism primarily invested in how the notions of authority and sovereignty are reformulated by and through blockchain technology.

Bitcoin is treated as an elongated case study, and provides numerous entry points into how digital technologies both alter and embody specific forms of authority and sovereignty. Not only is Bitcoin the first and most known blockchain, but its history is filled with rich anecdotes (like Barker's airport scene), political promises, and, as we shall see, highly suggestive internal contradictions.

Bitcoin's very emergence is, to this date, still associated with the myth of its creator. At the beginning of November in 2008, someone under the pseudonym of Satoshi Nakamoto posted a white paper in a cryptographic mailing list. The white paper introduced a system that claimed to have solved the double-spending problem[2] for digital currencies. Announced simply as a payment system, the

1 Subsequent iterations of this technology take other forms notoriously e.g. Ethereum's "smart contracts".

2 Bitcoin was not the first attempt towards creating a digital currency, but it was the first to successfully solve double-spending: how to avoid using the same duplicated digital file/coin/token to pay to more than one recipient, without resorting to a centralized

design introduced the idea of authenticating transactions of digital tokens in a shared ledger. The specific proposal, which combined widespread use cryptographic security keys with a public ledger, made counterfeit extremely difficult to achieve. The bigger the network and number of transactions, the more computationally demanding the authentication of transactions would become, and the less likely it would be to counterfeit them. The idea, paired with an early implementation,[3] attracted a small but dedicated group of enthusiasts, and then grew exponentially (Popper 2015). When the price of the currency, which started as fractions of cents per Bitcoin, achieved parity with the US dollar (USD) in February 2011, an article on Slashdot and a later piece on Forbes helped introduce Bitcoin into mainstream media (Wallace 2017). By May of the same year, the price was close to 10 USD. Two months later, the exchange market MtGox[4] was founded, and this turned out to be one of the most controversial events in Bitcoin's history. Speculation on the currency was paired with the proliferation of other exchange markets, and by the end of that year bitcoin reached 20 USD. This was the year that the cryptocurrency was first seriously considered as a payment system; one with the capacity to bypass economic censorship and facilitate illegal activities. In March 2011, Wikileaks started accepting donations in bitcoins, and around the same time the Electronic Frontier Foundation (EFF) also experimented with it. This year also saw the beginning of the Silk Road,[5] which used Bitcoin to facilitate payments. Regular media attention, huge speculations on price, concerns from numerous financial regulators, its associations with criminal activities, and general intrigue surrounding the ontological peculiarity of this money-artefact, all contributed to the swift growing of Bitcoin from 2010 to 2013.

It was during this time that I became interested in Bitcoin. The term started to circulate the world of Free/Libre Open Source Software (FLOSS), which I followed as a Linux enthusiast. Without fully understanding its technical specificities, or what a proposal of a new type of currency entailed, I was

system or third-party.

3 The first version of the code was published only a few months after, in January 2009.

4 MtGox was an important element in the history of Bitcoin. By 2014 it handed 70% of all Bitcoin transactions, but filed for bankruptcy in the same year, after allegedly 850,000 were stolen from it. A recent investigation (Nilsson 2017) has proved that the exchange was insolvent since 2011, and the money was lost by different incidents that include thefts, money laundering, frauds, and mismanagement.

5 A black market that used the TOR project network to hide its website servers. The FBI shut down the website in 2013, and arrested the alleged founder and operator, Ross William Ulbricht.

immediately puzzled by its apparent open nature. The idea of redistributing control of a small part of the economy from central institutions to an extended share of stakeholders was appealing, especially in the general context of the financial crisis of 2008.[6] The promise of a new way to circumvent some of the failures of the current economic system, and to distribute the performance of authority in it, generated a lot of excitement.

Like the steam-powered machines of the Industrial Revolution, Bitcoin is a technological artefact associated with changes in the configuration of the social landscape. But, and very much like steam, the scope and form of Bitcoin's machinery is clouded by an expanding rhetoric. What is commonly referred as steam is a mist of droplets of condensed vapour; steam as the gas state of water is invisible to the human eye. Likewise, blockchain technology is surrounded by the vaporous rhetoric of *the Blockchain*. Thus, my attention turned to the configuration of the Bitcoin machine, and how relates to the utopian dimensions that surrounds it. This research is interested in how the machine works, in the technical underpinning of the blockchain, and what kind of politics is unleashed in its performance. It tries to make sense of the vapour, out of the steam: what do the technical conditions of possibility —the material pieces and infrastructure— tell us about the political metaphors that encircle Bitcoin? And vice versa: What kind of political visions fed the assemblage of the machine? The thesis is thus overarched by different notions of "utopia", which, I argue, are manifested in different empirical contexts and elements of the Bitcoin blockchain. Specifically, I consider utopia as: paradox, ideal, no-place, and imagined governance. Different understandings of authority are highlighted and made comprehensible through this utopian arch. What I come to argue, however, is that the main characteristic of Bitcoin is its unique outsourcing of authority, from previous political models, to the legitimation of computational performance. I push this idea towards a theoretical position, and develop a critical account of Bitcoin's power dynamics, relying primarily on the figures of Empire (Hardt and Negri 2001), Protocol (Galloway 2004), and Stack (Bratton 2016).

The specific literature on Bitcoin has grown substantially in the last few years. The majority of academic research is dominated by the fields of Computer

6 And in particular because I come from a country where state institutions are normally associated with a high level of corruption. Mexico's average in the Corruptions Perception Index from 2102 to 2016 is 32.8/100 (Transparency International 2016).

Science and Economics. The literature can be roughly divided in introductory pieces, struggles for a financial definition, regulatory concerns, insights into the price variations, forked projects and improvements for the protocol, mining, and general security of the system. One of the earliest scholarly pieces provides new schemes to incentivize information propagation between nodes in the Bitcoin network (Babaioff et al. 2012). It is also common to find studies concerned with perceived flaws regarding Bitcoin's capacity for anonymization, its user privacy evaluations, or transaction dynamics. Relevant examples include Biryukov et al. (2014), who unmasks Bitcoin users by linking pseudonyms (or wallet addresses) to the IP addresses of the origin of the transactions. Concerns around the privacy of the system are shared by Androulaki et al. (2013), who build a simulator of a Bitcoin network to analyse privacy provisions. Meiklejohn et al. (2013) have analysed the flow of payments until April 2013, and successfully identified interactions between major institutions (for example, between MtGox and Satoshi Dice, a gambling platform). Many of these studies are not motivated to de-anonymize users in the system, but to warn against expectations that anonymity is assured (Reid and Harrigan 2013, 3); to improve the protocol with strengthened anonymity (Saxena, Misra, and Dhar 2014; Androulaki and Karame 2014); or revise associated software, such as wallets (Vasek, Thornton, and Moore 2014; Verbücheln 2015). Early research is also concerned with the categorization of Bitcoin as money or a different kind of asset, commodity, currency, financials tool, etc (Surda 2012; Mittal 2012; Selgin 2015; Bergstra and de Leeuw 2013a; Bergstra and de Leeuw 2013b); with specific concerns of money laundering through this system (Stokes 2012; Moser, Bohme, and Breuker 2013; Fortuna, Holtz, and Neff 2013); and discussions regarding variations in price (Wandery 2014; Kaminski and Gloor 2014; Shah and Zhang 2014).

Research on the social characteristics embedded in the production, usage and effects of the device is comparatively smaller. Examples of research within the social sciences include the theorization of Bitcoin infrastructure's affordances (O'Dwyer 2015; DuPont 2017; Maurer, Nelms, and Swartz 2013; Swartz 2017), the political demographics of its community (Smyth 2014a), and critiques of the ideologies associated with their communities (Jeong 2013) (Scott 2014). Maurer, Nelms, and Swartz (2013, 215) picks up on the idea of the railroad system as the 'rails' of money infrastructures to reflect on contemporary telecommunications

companies as the *pipes* of Bitcoin. He argues Bitcoin is a phenomenon where both the token and the rail have collapsed into one in the form of the blockchain. Together with his colleagues, Maurer also expands on the semiotics on Bitcoin and its rethinking of privacy, labor, and value debates (Maurer, Nelms, and Swartz 2013). Other studies (Smyth 2014a; Smyth 2014b) show that there was a strong diversity among the people surrounding cryptocurrencies and propose to address the blockchain as an entire cryptocoin ecosystem, composed with actors with different motivations, backgrounds and reactions, rather than as a unified community. Smyth's dataset is drawn upon later in this study (Bohr and Bashir 2014) to correlate statistically political positions and roles within the ecosystem (e.g. correlation of a libertarian stance and programmers).

A smaller set of social research differentiates from previous works through adopting a more critical point of view of blockchains. Scott (2014), who emphasizes that the digital-anonymous-decentralized-ledger systems are not by themselves a guarantee of good use, or of the flourishing of community dynamics within society. Blockchain currencies can be alternatives to current economic systems, without being progressive or socially desirable (Scott 2016a). Golumbia (2016) identifies a strong libertarian ideology within Bitcoin's design and ecosystem. In the same vein, Jeong (2013) argues against the alleged 'apolitical' nature of the project and claims that libertarian and metallist philosophies have shaped the cryptocurrency. O'Dwyer (2012) introduces a discussion around the infrastructure of Bitcoin, and argues that its decentralization does not necessarily correlate with a reduction of the mechanics of domination. She posits that despite the current centralization of Bitcoin's infrastructure by mining pools, the broad technology of the blockchain still carries the potential of a being a tool for a social networked operation (O'Dwyer 2015). Likewise, Dupont (n.d.) identifies within the cryptographic affordances of Bitcoin a "new weapon" of the control society (Deleuze 1992), and for the control of economic activity specifically. Swartz (2017) has argued that the majority of the investment in the blockchain currently relies on projects that seek to aid taming the complexity of modern finance, but not to replace it. This last group of authors informs much of what follows and my own position has benefited from a productive dialogue with them.

While for much of this last body of work the monetary nature of Bitcoin is an implicit ground, my research is not driven by the economic nature of Bitcoin. I

focus my attention on the power dynamics working in the design and performance of the Bitcoin blockchain, and only to economic considerations when they are derived from the former. There are currently no full-length monographs which approach Bitcoin as a digital media object, while also considering the rhetoric that surrounds it. Thus, this thesis offers an original research position that draws together questions of materiality, ownership, governance, territoriality, and the performance of the machine. This research also identifies the inconsistencies between the "steam" and the "vapour" produced by the Bitcoin machine.

The recursive readings of "utopia" in each chapter signal Bitcoin's internal contradictions: the overlapping notions of public and private in the production process; the struggle between privacy and decentralization on the one hand, and the free market and competition on the other; the territorial ties with the state paralleled with the affirmation of a sovereign space; and the circularity of the technical determinism of Bitcoin's performance and the social construction of its design. The configuration of the technical object and the political struggles embedded with it, shed light on a broader momentum of the ubiquitous computational ontologies of our times. The discussion highlighted by this thesis reveals a state of affairs that goes beyond the blockchain as a particular technology, and contributes to contemporary understandings of the networked production of knowledge and value. The argument I develop about the outsourcing of authority roles to automated non-humans is not unique to Bitcoin, and is shared with a culture constructed around the myth of the algorithm. Blockchains adhere to and help perpetuate these cultural myths.

Chapter Plan

The thesis contains five chapters. Chapter One addresses the key process of production, mining, and how this relates to a particular computational notion of authority. The chapter develops a theoretical argument derived from Bitcoin's technical function. It raises the question of why authority is a particularly complicated issue in Bitcoin due to lack of a clear founder, and due to its open organizational model of development. I argue that the project's undefined hierarchy opens up *a vacuum of authority*, which is partially but not entirely fulfilled by different groups of actors, and which is further defined by each group's

relation with the figure of the state. These relations can be professedly antagonistic, alternative to already existing state administrative institutions, or seeking validation and incorporation within the existing state apparatus. These groups have contested ends, and yet gather their not-so-easily reconcilable stances under the same banner of blockchain technology. In order to understand the nuances of these divisions, the chapter distinguishes between the concept of "decentralization" and "public" in relation to blockchain technology. A second section offers a detailed view on the mining process. This section presents the computational logic embedded in the production model, and shows how this logic is materially expressed. I use the correlated notions of "waste" and "abundance" to explore how the hardware's consumption of energy, which is built into the design of Bitcoin's protocol, relates to the political ideas attached to this design.

At this point, the production of authority in Bitcoin by computational means becomes a key element of my argument and the basis from which I proceed. I claim that this specific kind of production works beyond its technical purposes and becomes a tool for legitimation. Accountability in Bitcoin does not come from an external source, as opposed to current production of fiat money, which is legitimized by an external authority (i.e. the state, through central or commercial banks). On the contrary, I argue that the legitimacy of the system is folded within the system itself: due to the particular nature of Bitcoin as open, distributed, and independent to state and corporations system, its legitimation is held within its own automated management of the production, and measured by the successful performance of automated validations in exchanged communications. The chapter ends by stressing the coexistence and particular enactment of the public and the private in the production of bitcoins: the system effectively produces private non-reproducible tokens with the use of a public ledger reproduced all along the network. I identify that it is this folded coexistence what equally fuels dissimilar political projects. The private properties of production feed both the imaginations of private, frictionless exchange for the liberal-oriented economies on the one hand; and of shared means of production for cooperative networks, on the other. As I will suggest, the unique production model in Bitcoin feeds very different political positions.

In Chapter Two, I present the methods deployed throughout the work. I outline the methodological approach of using digital methods to make sense of

digital objects. The chapter also clarifies the crucial use of “the political” in this work. I delineate both my methodologies and use of the political in relation to previous literature. In particular, I follow the fields of Media Theory and Science and Technology Studies, both of which are informed by (or at least compatible with) a Foucaldian perspective on knowledge. However, this chapter is also used to clarify where my work diverges from the previous literature. Finally, I stress my position on what I consider to be a critical issue regarding the use of digital methods: recursivity.

Chapter Three builds an historical account of the blockchain, from the seventies to just before the appearance of Bitcoin. Taking a cue from Tung-Hui Hu (2016) notion of prehistory, the chapter takes some of the pieces of the Bitcoin machine and trace their emergence and development. Like Hu, I am interested in the material infrastructure embodied in the machine, but also in the extended metaphor which develops around it. This query is also inspired by the field of Media Archaeology, but does not rely on the medium-specificity of that approach. While Bitcoin as a digital object catalyses and conjoins these historical threads, the threads observed along its prehistory are not exclusive to Bitcoin. Furthermore, the chapter observes the political context or ideologies associated with these technological pieces. Specifically, I identify three trajectories joined by two events. First, a trajectory concerned with secure communications, in which many of the cryptographic techniques used by Bitcoin, directly or as a later iteration, were developed. The second trajectory appends an explicit discourse and political tone to cryptography. This trajectory identifies a political investment on the democratic use of cryptographic techniques expressed, which unfolds through an analysis of a number of manifestos. In the manifestos, code is reformulated as a political praxis, and in direct confrontation with the state as the (then) sole executor of these technologies (previously existent only in military contexts). Plenty of the concerns voiced at this time became prevalent, at least rhetorically, in the configuration and evolution of both the internet and the blockchain. Finally, a third pre-historical trajectory starts to imagine the use of cryptography for the creation of digital money or digital payments. It implicitly suggests the possibility of using technology to replace the institutional strongholds of the nation-state economy.

However, this last trajectory blends the political discourse of privacy with that of the free exchange of assets, and thus, I shall argue, obfuscates the main

rationale for antagonism towards the state. That is, while the topics of privacy and decentralization may coexist with free market and competition, quite different scenarios can be developed depending on which is prioritized as an end, and which as a means. I will later argue (Chapter Five) that this ambiguous merging explains not only the multiplicity of the projects associated with the blockchain, but one of the biggest controversies in Bitcoin's development. The utopian envisioning of cryptography technology presented in this chapter, offers an historical account of the development of blockchain technology (and related metaphors) into dissimilar political ends. It also underpins part of the ideal execution associated with code. While this chapter argues that the Blockchain does enhance the role of code —and code's performativity— as an authority within governance arrangements, it also stresses the distance between code performance and the actual achievement of ideal political scenarios.

Chapter Four looks into the spatial configuration of Bitcoin's network. It offers an answer to the question of where the blockchain is located and does so through an empirical analysis of the network's nodes. This exploration offers a new way of understanding Bitcoin's geographical characteristics and importantly, reveals the inadequacy of a territorially-based approach to deal with its spatiality. This lack suggests the need for a geo-political conception of the blockchain that exceeds the nation-state and I draw upon Benjamin Bratton's notion of the Stack in order to advance such an understanding (Bratton 2016). The chapter opens with a commentary on power, framed as sovereign control within territorial boundaries. I then comment on some of the literature regarding the geographical reconfigurations allowed by the internet. Considering that all blockchains are underpinned by the geographical characteristics of the internet, they inherit a great part of its technical and rhetorical reformulation as cyberspace. The promise of a place unbound by territory became influential during the 90s (this is directly related to the trajectory of manifestos in Chapter Three), but much of this vision was eroded as it became clear that the internet was not immune to territorial control. The blockchains are, among other things, a reaction towards this territorial control. They are explicitly designed to not be affected by territory in terms of performance. The utopian element of the cyberspace as a no-place is resurrected by both the imaginary and the technical design of the blockchain. I show that Bitcoin oscillates between being subject of location and, at the same time, performing its spatiality in a no-place.

In order to illustrate this apparent contradiction, I track the way the network behaved in relation to space during a determined period of six months in 2015. The tracking of the network behaviour shows that its nodes cluster in identifiable regions. Thus, I argue that the network is locatable and concentrates in certain regions. However, the notion of territory is non-essential for the performance of the network. Following Andrew Barry (2001; 2006) and Saskia Sassen (2006) work, I argue that the relation between territories (as state-controlled planar geographies) and the Bitcoin space is made mostly through standardization processes. Nonetheless, I stress that the way this network works and makes sense of its space is not directly subjected to territorial arrangements or state-determinations. On the contrary, part of the imaginary related to the frictionless exchange promised by this machine is the minimization of the territory as a technology of power. The chapter ends by arguing that a better understanding of the network requires a non-planar approach. Thus, the post-Westphalian figure of the Stack offers a better model to understand the political geographies of Bitcoin and other blockchains.

The final chapter focuses on the organisational dynamics of Bitcoin as an open (source) project, paying particular attention to developments after the disappearance of Nakamoto (the creator). Unlike previous chapters, which focused on different sides of its computational performance, Chapter Five describes the internal decision-making involved in the development of its computational workings. The chapter starts with an overview of different projects that attempt to integrate blockchain protocols into democratic processes. The final notion of utopia as “governance through other means” is expressed by these projects. A considerable number of blockchain projects are an investment in using technology to overcome perceived flaws in human interactions and traditional organizational forms. The brief discussion of these utopian projects on improving democracy opens the way to investigating the internal democratic processes in around the development of the Bitcoin protocol. Like other Open Source Software projects (OSS), the development of Bitcoin has produced clear guidelines for proposals, voting, responsibilities, and cooperation for deployment. I start by portraying the specific strategies for consensus inscribed in the OSS nature of Bitcoin. Everyone is free to propose a change to the code, and all proposals go through the same procedure. Ideally, most disagreements are discussed and settled through these

strategies. In a worst-case scenario, the possibility of forking —splitting or replicating the code to develop another project, which may or may not compete with the original— offers a diplomatic way to deal with strong disagreements.

However, I will argue that the combination of Bitcoin as an OSS and as a scarce economic artefact complicates the strategies for democratic consensus. The chapter follows a well-known controversy in the history of Bitcoin that persisted, unresolved, despite the refined procedures for reaching agreement in the modifications of the code. The controversy centred on how to scale the network capacity of the Bitcoin to process transactions. While an immediate solution —to expand the blocks' capacity in the chain— was technically easy to implement, it entailed a clash in the ideological positions of the, until then, fairly cohesive community of developers. I follow the rationale for and against this particular solution for scaling, and identify key actors in the discussion. The reconstruction of the controversy not only clarifies the scope of the disagreement, it also evinces what is at stake in the larger history of Bitcoin as a digital and political artefact. I argue that the developers —and by extension the community— were divided by the resolution of, on the one hand, the utopian ends of a frictionless free market, and on the other, the also utopian ends of decentralization. While these utopian ends were previously indistinguishable, the block-scaling controversy made clear that even if they were initially not contradictory, opting for one or the other ultimately meant to choose between significantly different technical developments.

Through these diverse inquiries into the Bitcoin blockchain, this thesis contributes to the discussions on how technology rearranges social structures of power. The analysis of this current phenomenon offers a detailed overview of the socio-technical operation of technology devices from a diversity of approaches, and provides empirical evidence on the ontological and epistemological scope of this operation. It also contributes to develop an appropriate political theory to think about new technologies and their impact, which takes into account the specificities, limitations, and affordances of blockchains' technical grammar. The discussion of power dynamics in the times of *planetary-scale computation* (in Bratton terms), provides a fertile ground to extend knowledge on the relations between power and technology. This thesis contributes to this discussion by providing an account of the novel technology embodied in blockchains within the context of power apparatuses.

Chapter 1: Outsourcing Authority to Algorithmic Production

The £50 note is rarely seen in the wild. Cash is an endangered animal in the United Kingdom (Jones 2017), it is easier to find whichever combination of plastic and silicon on day-to-day transactions. Even without considering the gradual transition to a “cashless society” (Scott 2016b), fifties are a rarity in the sterling family. Whoever has placed his or her eyes on this elusive note may have noted the steam engine featured on one of its sides. Introduced in 2011, the design praised the archetypal machine of the industrial revolution that changed the landscape of the country and the fate of the world. The note includes the figure of James Watt, inventor of the steam engine, and of Matthew Bolton, his business partner. On the note, a Bolton quote reads: “I sell here, Sir, what all the world desires to have - POWER”. The quote is compelling for a number of reasons. First, it implicitly states the universal, borderless, nature of power, and exemplifies the globalizing tendency of industrial and modern capitalism. Second, that power is a product on sale, it is transitional, for the right price. Third, it is embodied in a machine: what confers power is not what is produced but the process, the industrial work itself. Finally, the former messages are enveloped in a square of flowing fiat paper, itself a medium identified with power.

Bolton was the co-founder of the lunar society, which gathered industrials and intellectuals of the so-called Midlands Enlightenment. He describes the benefits of his coinage presses as follows: “It will coin much faster, with greater ease, with fewer persons, for less expense, and more beautiful than any other machinery ever used for coining (...) The machine keeps an account of the number of pieces struck which cannot be altered from the truth by any of the persons employed.” (Delieb 1971). Although these words are around 200 years old, Bolton could very well be talking about the affordances of the bitcoin machinery. Like the steam engine, the first implementation of blockchain technology has been the basis for promises of global democratization, abundance, renewed economic trust,

elegance, and economic freedom. Indeed, one finds too many promises, attached to different and often incompatible projects, made under the same banner: anarcho-capitalist untraceable money; perfect industrial-compatible standards; collaborative action coordination; digital citizenships for the ultramodern state; a new distributed internet aiming to replace its late re-centralized platformisation; the list goes on. Like any other myth associated with solutionism (Morozov 2013), blockchains do bring exciting and diverse enhancements, but not for everyone. Will this technology ease the worst excesses of the current economic system? Do its disruptive qualities enable a tweak of the system towards more social ends? Will it enhance economic participation and revitalise struggling communities? Which heads of this Blockchain chimera are real, and which have a virtual existence? And how is it possible that the same piece of technology generates remarkably different dreams and realities?

This chapter offers an explanation for the sometimes incompatible diversity of this technology. It is grounded on the very particular position regarding an apparent lack of authority in Bitcoin. My reading of authority is close to Max Weber (1991) bureaucratic or *rational* authority, which is recognized as the one coming from a normative order, and *traditional* authority, which is an inherited type of domination. I will argue that while the design of Bitcoin strongly depends on normative grounds – more at the development level of open software projects, than in relation to state regulations – the performative element of the technical system displaces control from traditional bureaucratic institutions towards the technical operation of the system. To begin with, normative figures are elusive in Bitcoin's ecosystem. Neither sovereign (Foucault 1982) nor disciplinary (Foucault 2012) subjects or institutions are clearly situated. The execution of decisions in Bitcoin is not as easy to locate as in other projects due to several facts: the disappearance of the founder, its open nature, and an undefined and extended community, to name a few. This vacuum of a clear authority opens up a space to be disputed by different groups with variable degrees of success. I focus on three groups that claim this space, and which are in great part defined by their relation with the figure of the state: a group identified with libertarian ideals, which plays an antagonistic role towards state control of assets and identities; a group that sees in the blockchain the possibility for alternative approaches to democracy, thus the promise to distribute state control; and a group that sees the figure of the

state as an important player in the incorporation of this technology into platforms to improve financial markets. Public blockchains, however, fit partially but not entirely into these groups. The vacuum of authority obfuscates how power is performed, and feeds the idea of the blockchain with dissimilar utopian outcomes.

The second part of the chapter provides an argument that locates authority into the system of production itself. Here I argue that the specificity of production in public blockchains encapsulates, very much like the steam engine, the emergence of a power structure. This structure is based on the computational logic that underpins the process of *mining*, which folds exchange (as accumulation of transactions into blocks) and production (as transactions into blocks are successfully accumulated) into a single action. I explain thoroughly how this procedure works, and argue that it is based on the idea of a superabundance of computational resources. Hardware consumption in the form of algorithms transforms energy and intensive calculation into an efficient and fully automated management system. The performance of the blockchain as a production machine takes the place of institutional authority. More than to a group outside the system, legitimation and accountability are primordially outsourced to the computational system or production itself. Both parts – the authority vacuum and the production of power – explain the paradoxical momentum of the discourse and actualities of the blockchain.

The first notion of utopia addresses this paradox: an unclear interplay between the public and the private. The latter embodied in the generation of a private digital token able to circulate almost seamlessly, thus expressing a liberal-oriented political goal; the former embodied in a shared network, performed by the work of a multitude (Hardt and Negri 2005). The design of the blockchain effectively combines a public structure to produce a private element. I argue that, paradoxically, this particular structure informs the rhetoric of two different political positions. This association maintains the popular rhetoric surrounding the technology, an idea of a co-operative effort capable of securing private digital tokens. Numerous projects now and in the past decade have exploited this paradox to advertise the technological positivism of blockchains; however, there are scarce examples of projects that actually perform as a social co-operative effort. The coexistence of the public and the private in the blockchain is

anomalous insofar as it deceitfully feeds an empowerment discourse of collaboration and radical redistribution of power relations.

1.1 Enter the void: Power in the Absence of Authority

Bitcoin is, among other things, an open technological protocol. As such, it is ruled by a specific governance model of open software. Details on the successes and failures on this model applied to Bitcoin are presented in detail in the last chapter of this work. There, I show how the notion of Bitcoin as a financial product prevents the use of classic open source strategic actions. I also stress the lack of a clear leadership in the project. While the early years benefited from the *presence* of a creator —even if always under the veil of anonymity— his absence was followed by diffused and never completely compelling leadership roles within the nascent Bitcoin communities. Satoshi Nakamoto, the pseudonym for the creator or group that envisioned Bitcoin and presented the first version of the software, progressively lost contact with the rest of the developers, and finally disconnected from any discussion at the end of 2010. His identity is unknown to this date. The attempts to offset Nakamoto's disappearance with an institution (i.e. the Bitcoin Foundation) have soundly failed. The foundation's purpose was to "standardize, protect and promote the use of bitcoin" (Matonis 2017). Its original board of directors included figures that became highly controversial and thus affected their leadership roles.[7] While the foundation exists to this date (with a complete different set of board members), it does not play a central role in the extended community. In a way, the system was designed to be *un-proprietary*, to belong to no-one, which does not immediately translate to belonging to everyone, as much as the surrounding rhetoric of decentralization claims. I will expand on what is at stake in being a system that is not owned in the second part of this chapter. As an open project, Bitcoin's definitions of ownership and leadership differ from states and corporations, and after Nakamoto's disappearance, authority within it became hazy to say the least.

7 Two of the six original board members were related to criminal activity: Charlie Shrem, the founder of *Bitinstant*, was sentenced to two years of prison (2014-2106) for aiding the operation of the *Silk Road* black market. Mark Karpeles, the CEO of the major bitcoin exchange *MtGox*, was arrested in Japan in 2015 and charged of embezzlement. Mtgox became famous for loosing 850 000 bitcoins from his customers, valued 450 million USD at the time (and almost 3.5 billion USD at September 18th 2017). At this moment, he is released on bail.

The vacuum analogy works to invoke a seemingly void space, that is, a lack of authority. Even if emphatically surrounded and partly inhabited by abstract figures like that of the Community, the Corporation, or the State (embodied in specific instances as per case: the main developers, Blockstream, or the People's Bank of China), neither of them plays the role of *de facto* ruler. If any, each maintains authority in their own specific blockchain manifestation. The hard-fork controversy, which I consider in Chapter Five, made evident the fragmentation of the so-called community. In that chapter, I narrate this break attentively to show how Bitcoin, the archetype of decentralized trust, failed to decentralize community driven design.

A second meaning of vacuum is of a vortice that attracts surrounding matter. The Bitcoin ecosystem maintained a fuzzy relationship with different institutions. Part of its community was at times confrontational with state regulation, for example, while others were open to negotiations with state actors. A position for and against private financial corporations or tech giants was never totally settled either (but a look at the evolution of these relations is revealing). Some institutions, including old and new financial technologies corporations (e.g. *IBM Blockchain Solutions*), occupied the void with more success than others. The vacuum of authority attracted different players and reconfigured the power and influence relations not only for Bitcoin, but also for the numerous iterations of blockchain technology that followed.

The chimerical status of diffuse governance, the lack of infrastructural ownership, and production of digital private property, sheds light on the current multiplicity and incoherence between Blockchain projects. This becomes more evident when the position of each group in relation to centralized authority institutions is brought into question. In order to open an inquiry of how authority is performed in these particular systems, I will present three different categories of blockchain endeavours based on their relation with the state. Each group is an abstract generalization of more complex empirical nuances, however, this strategy will allow me to clearly distinguish one from each other. A straightforward research question guiding this section is then: are blockchains aiming to destroy, replace, or reinforce traditional state institutions? The answer to such a question may be radically diverse depending on which interested party is addressed. Each interpretation feeds a different set of projects that supports distinct ideologies

present in the blockchain: *freedom* (destruction of the state), *cooperation* (replacement of the state), *in-corporation* (reinforcement of the state). But not all are equally vibrant, funded, or populated. Thus, they have different degrees of reality.

Political Vortices: Freedom, Cooperation, and In-corporation

In 2014, Lui Smyth, an anthropology PhD student, conducted a survey directed to the (then) relatively small Bitcoin user community. Based on 300 answers, his research showed the political compass of the community through some basic demographics: "one quarter libertarian, matched by a quarter liberal, and a quarter more left-wing, with a few smaller groups of other political identities" (Smyth 2014a). The "left wing" refers to the users that saw themselves as 'socialists', and the "other political identities" include communist, theocratic, anarchist, and conservative, among others. The Bitcoin project was initially supported by a combination of tech savvy, liberal, and libertarian-oriented actors. Many saw an opportunity to gain economic sovereignty from the state via the distributed ledger. The enthusiasm for pursuing the free subject through technological artefacts follows Foucault's (1982) notion of *governmentality*, a form were a governing power is exercised after traditionally modern sovereignity, i.e. outside of the view of the state. Power then is exercised through dispersed technical strategies (Foucault 1980a). The many possibilities of implementations of economic self-governance through technology made this a golden age for envisioning and implementing the blockchain as cryptocurrencies.[8]

The Bitcoin project can be read as a libertarian or anarchic model, which points to different readings of economic and social 'freedom'. If not all, a great majority of its expressions was categorically against the state as a regulative authority of law and exchange of value. These "visions of a techno-leviathan," as described by Brett Scott,

8 While there is no question that a good degree of diverse political positions exist among Bitcoin enthusiasts, there was a substantial libertarian formations surrounding the system. See for example (Popper 2015) for a close narration of the people invested with Bitcoin's early years; and (Golumbia 2016) for a critical perspective on the heavily oriented libertarian ideology of the project design and ecosystem.

> appeal[ed] to people who wish to devolve power away from banks by introducing more diversity into the monetary system. Those with a left-wing anarchist bent, who perceive the state and banking sector as representing the same elite interests, may recognise in it the potential for collective direct democratic governance of currency. It has really appealed, though, to conservative libertarians who perceive it as a commodity-like currency, free from the evils of the central bank and regulation (Scott 2014).

The space where Blockchain technology proposed to settle was in the realm of economics at first, but as Scott argues, the use of blockchain technologies to disrupt other kinds of centralized institutions within the state, like copyright law, DNS management or even democratic tools like voting systems, quickly followed. An interesting finding of Smyth's survey was that despite the main use of blockchains as a disruptive currency, the average Bitcoin enthusiast was more driven by the political sentiment that the system represented than by actual monetization: many didn't "talk about their stash as an asset, but rather as a shared interest" (Smyth 2014a). This detail will become particularly relevant as the finance industry gradually overshadowed the libertarian community in the ecosystem in the years that followed. Unlike the early years, the system would become less relevant for their political values and more for their qualities as a fluid financial asset.

From the initial explosion of *altcoins* that followed Bitcoin, only a few surviving examples remain today, and most of them act as cryptocurrencies patching security and protocol issues of its predecessor. Some notable examples went beyond that, like *Namecoin*, which (still) attempts to distribute one of the historically centralized cogs of the Internet, the Domain Name System. The blockchain fuelled the imagination of the anarchist dreamer. It appeared that for any task done by an institutional centralized authority, there was a small project in the Bitcoin ecosystem seeking to replace it. But attempts like Namecoin have become a rarity. One of the biggest contemporary projects representing the early libertarian positions – primarily concerned to get rid of state involvement in the production and exchange of money – can be found in *Zcash*, a fully anonymous cryptocurrency aimed to mend the pseudonymity holes that enable new techniques for tracking and identifying Bitcoin users. However, the explicit

concerns for privacy and freedom have been surpassed by financially-oriented goals[9].

A minor (but familiar) second category of the blockchain enthusiast, gathers a group that observes the blockchain with criticism and creative curiosity. This very loose group gathers researchers, artists, and activists.[10] Internally diverse, but hardly associated or driven with the libertarian ideology of the first category or the profit-seeking motor of the financial technology industry, this category is less antagonist to the state. Instead, it has an invested interest in tweaking the shortcomings of the technology, stressing its implicit ideologies, or playing with their cognitive and affective affordances.

This cluster of projects is also concerned with improving democratic participation, creating new forms of enhanced horizontal organization, or questioning traditional notions of money, in many cases through provocation. This is the promised moment of distributed collaboration. This point of view is undoubtedly invested in deconstructing the relation with the state, but rarely with the explicit goal of eradicating its institutions. For example, *Commoncoin*, envisioned by Tiziana Terranova and Andrea Fumagalli, was inspired by community-based policies, such as minimal wage, basic income, negative interest and generative transactions (Terranova and Fumagalli 2015). In a similar fashion, Steve Huckle and Martin White (2016), on the premise that the tokens ('native digital assets') circulating through blockchains can be linked to any social construct of value, offer tentative applications of the technology for socialist-driven projects.

As promising as these projects sound, however, they are often imaginative exercises. That is the case with the former examples. They offer no continuity, are minimally developed, or have no implementation at all. Radical social ideas for the Blockchain remain ideas. This is a frequently recurring symptom. There are also arguably weaker versions of a truly communitarian system currently deployed and these can be considered experiments in progress, like *Swarm* (http://swarm.fund/), the crowdfunding attempt that makes use of 'crypto-equity', or *Steemit* (http://steemit.com/), a social network that rewards creators for their

9 In Chapter Three I argue that these concerns are relevant as a basis for the blockchain both as a technical object and as a metaphor. Nonetheless, projects with the ultimate goal of perfecting privacy in the blockchain are a minority in the current ecosystem.

10 The Moneylab conference and associated publications (Lovink, Tkacz, and Vries 2015; Gloerich and de Vries 2018) gathers this particular positioning.

content. Both are blockchain-based working examples that attempt to change current distribution models. However, they are particularly recent, and thus it is difficult to predict their success. It would be reasonable to expect minimal adoption, progress and even their inevitable demise, especially when compared to their finance-oriented counterparts. Brett Scott posits the correct question in the title of a working paper for the United Nations Research Institute for Social Development (UNRISD) workshop: *How can cryptocurrency and blockchain technology play a role in building social and solidarity finance?* (Scott 2016a). The outcome of Scott's excellent paper is, perhaps unsurprisingly, that the question remains unanswered.

This cluster is relevant from a politically progressive point of view, but the category is more than modest in the vast ecosystem of the blockchain. This cluster is out of sight of, or irrelevant for the heavily financed projects. However, its relevance relies more on the role it plays in maintaining at the same time a critical position and the conviction that blockchains are pieces capable of social solidarity enhancement. As I will argue, these imaginaries of the potential of the technology are a direct consequence of the production system of public blockchains, and play a significant role in the endurance of its utopian promises.

Finally, the fintech industry, a corporate chimera itself, has received with open arms the distributed ledger technology. *This is the booming age of private blockchains*. Differentiated from the state, but not as its antagonist, the industry has slowly integrated blockchains into their own financial models and pushed for standards that will allow the industry to exploit the technology under certified and legal frameworks.

This interest produces an interesting contrast with Bitcoin's early years. Smyth's 2014 survey also measured the most trusted groups in the eyes of the bitcoiner. Trust at the time was first of all placed in the "core developers", followed closely by "merchants" (Smyth 2014b). The last position was occupied by "financial companies". The Bitcoin enthusiasts even showed more trust in the "governments" category, something remarkable considering the explicit opposition of the libertarian population among them. Smyth reminds us that "to understand the sometimes slippery ethics of Bitcoin, we have to account [...] for its perceived dialectical opponent, an entrenched and indifferent economic elite" (Smyth 2014a).

If the discursive life of Bitcoin and other blockchains is characterized by being confrontational to the state (although in practice its survival and evolution has been made possible by a smoother relation), the relation with tech conglomerates is not obvious (this occupies a middle point in the trust scale along with alternative cryptocurrencies developers). The extended debates I consider in Chapter Five show this complex relationship as an early sign of the community breakup. Peter Todd and Mike Hearn (see Chapter Five), both early developers and enthusiasts of the cryptocurrency, play the roles of opposing forces regarding the subtle ideological differences that fuelled the "scaling debate". These differences are grounded, among other things, on the stance taken by the Bitcoin project in relation to tech giants and the financial industry. During the early stages of the debate, more than once Peter Todd made personal attacks to Mike Hearn for being a Google employee:

> You come from Google, a place of massive centralized server farms controlled by one company. Google's services work pretty well - centralization can have benefits - but many of us feel that goes down a very dangerous path. It's easy to see how a world where blocks are sufficiently large that only well funded pools with highly visible high-speed internet connections can lead to government and large businesses controlling Bitcoin ('Soft Block Size Limit Reached, Action Required by YOU' 2013).
>
> What does Mike's employer, Google, stand to gain from large blocks that only large companies can afford to process and validate? What does Google stand to gain from a system where every last transaction is recorded on a public blockchain, ripe for data mining? Mike after all works for a company that has a "real names" policy and actively tries to ensure users can-not use its services anonymously. Keep in mind Mike is also being paid by Google to work on Bitcoin; 20% time projects, while often speculative, are approved by management and must relate to Google's business interests in some fashion ('Funding of Network Security with Infinite Block Sizes' 2013).

Hearn would eventually leave Google to focus on Bitcoin development, and thereafter would leave the Bitcoin project to work for a private Blockchain startup. Many of the supporters of block scaling, like Hearn, aimed to see Bitcoin as a competitive network, more than an elusive one. Hearn was convinced on the virtues of "basic capitalism" as a general supplier. When confronted by another user ("nagato") on his optimist view on the power of capitalism, and how it has

failed to provide nutrition and energy for everyone, Hearn answers: “It has actually. The world produces a surplus of food (see the notorious EU ‘cheese mountains and wine lakes’). People still starve, but that's usually due to political problems (food can't get to where it's needed), not because we don't know how to feed everyone. (…) [and regarding internet] Really? I get free internet every time I go to Starbucks.” (‘Soft Block Size Limit Reached, Action Required by YOU’ 2013).[11] Technology corporations flawlessly flirted with blockchain technology, but for some enthusiasts the unique characteristics of common ownership (or lack of ownership) of the distributed system is what is quintessential to it. This means that although assets derived from the blockchain can be owned and commercialized through or outside the Blockchain, the technology itself (at least in the case of Bitcoin) cannot. From this point of view, it behaves much like any open source (Raymond 2008) technology in the last 20 years: it has a symbiotic relationship with corporate tech business, both contributing to and receiving benefits from it. As long as the mantra of decentralization was on the table, tech companies did not pose a threat.

But times have changed since 2014. The void of authority left by Nakamoto was partially filled with a few contrasting groups, while any effective influence on the design of competing blockchains was limited to a few voices. While the controversy stagnated and the ideological differences became more real, the dream of Bitcoin governance as an ideal democratization of technology faded. Individuals turned into companies (e.g. many of the core developers were hired by Blockstream). Tom Redshaw recently contested that Bitcoin can be considered a democratic appropriation of technology (Redshaw 2017), for the most part because a subgroup overriding power over a certain technology is far from democratic. While the fork controversy slowly grew, the fintech industry started developing its own alternative and personalized blockchains. Redshaw identifies that even the libertarian community has started to be eclipsed by the financial sector presence, showing how an already existing set of institutions have taken command of a supposedly alternative tool. Subordinate actors, be they

11 It is hard to tell at which point Hearn is joking or being cynical. As the discussion continues, “nagato” tells Hearn that he probably supports unemployment benefits, which benefit less fortunate and get funded 'somehow'. The answer from Hearn is “Yes, I do support unemployment benefits. People who lost their job and die on the streets are annoying if you trip over them. A bit of tax is a reasonable price to pay for not having to jump over bodies all the time”(March 08, 2013).

libertarians, anarchists, or even a broader set of society, are unable to challenge the power structures of the finance industry and their conditions of supremacy, as long as no broad democratic models of technological design are put into practice.

Here the list of projects is vast and healthy. A majority of the investment currently relies on the many "incorporative" (Swartz 2017) blockchain projects that seek to aid taming the complexity of modern finance, not to replace it. An example is the *Nasdaq Private Market*, a blockchain implementation concerned to manage private shares of technology companies pre-IPO's: "The goal here is not to disintermediate the financial system, but to determine how to be better intermediaries" (Swartz 2017, 99). Another example is the *Hyperledger*, an open blockchain development project backed up by a long list of big institutions and corporations (IBM, the Linux Foundation, Cisco, Intel, JP Morgan, and Wells Fargo, to name only a few), which works to develop a secure blockchain framework for regulated industries.

Inherent Design and Public Blockchains

The three categories I have presented are neither exhaustive nor always exclusive. They all may present themselves as collaborative, for example. But their understanding of this notion has significant differences, which can even be in contradiction. They also focus their attention on different parts of the blockchain —e.g. security vs. efficiency. Their position in relation to the figure of authority represented by the state shows some of their irreconcilable differences. However, a future case-by-case study would show an interesting granularity. For the moment, they demonstrate how the speed of technology has been accompanied by different scenarios driven by dissimilar political positions and ends. Before delving into a discussion on their performance of authority in the second part of this chapter, I will question the role of decentralization in these devices. This will offer a sharper position to differentiate the former categories.

The politics of the blockchain as *incorporated fintech* and as *collaborative public projects* can be detected in the contemporary discussion of platforms. On the one hand, an already evolved notion of platform capitalism already surrounds us. Masked by the mild and ubiquitous term of the "sharing economy", a handful

of massive platforms fuelled by the Silicon Valley imagination shape our relation with other (eg. Uber, Facebook, Amazon, Airbnb, Google). On the other hand, a diverse movement to re-conceptualize and redistribute the affordances of platforms is gaining momentum (Scholz and Schneider 2017). In his analysis of the conundrums of the first kind of platforms, Nick Srnicek broadly defines platforms as digital infrastructures that facilitate interaction between groups (Srnicek 2016). Blockchain technology was envisioned to ease the exchange of digital pieces without the need of a central authority via the mediation of algorithms. In this sense, it shares the instrumental goals of other platforms and, like many data-driven ventures, works fairly well with the key functions of contemporary capitalism: advantage is given to the algorithm; it enables coordination and outsourcing of workers; allows the optimization of processes; low-margin goods are easily transformed into high-margin services; and data analysis generates more data (Srnicek 2016, 41–42). However, while public blockchains may join Srnicek's categories of capitalist platforms (in terms of *advertising*, *cloud*, *industrial*, and *product*, the platforms identified by Srnicek) with minimal caveats, they remain a *fata morgana* due to the lack of corporate ownership: even if the Bitcoin blockchain development is constrained by a loosely identifiable group, the blockchain as such is not 'owned' by any individual or institution in particular.

A key conceptual element to understand the malleability of the political position among blockchains is the distinction between public, distributed, and decentralized (Baran 1964). The organizational model of blockchains, for example, can be distributed while having different degrees of centralization. On the one hand, Bitcoin is an example of a public —as opposed to incorporative— distributed instance that becomes centralized in relation to the amount of computer power: a hypothetical cluster of computationally powerful machines located in a single room would effectively regulate the behaviour of the network, regardless of the number of less powerful machines distributed around the world.[12] On the other hand, the same distributed technology can be implemented in private blockchains, in which a defined institution or group can control and modify the basic rules of behaviour. An example of the latter is Linq, a private Nasdaq blockchain, aiming to provide private securities transactions ('Nasdaq Linq Enables First-Ever Private Securities Issuance Documented With Blockchain

12 The role of computer power in topological formation of the network is discussed in Chapter Four.

Technology (NASDAQ:NDAQ)' 2016). Like other private blockchains, the shareholders of the system are limited and deliberately selected. The system design of a distributed ledger remains, but the centralization and ownership differs on each blockchain. Blockchains may be public or private, centralized or distributed, or any combination of the former.

Thus, I dispute the common misconception that the main characteristic of the blockchain is to be inherently decentralized and public. What is more, I argue that this strongly attached association is responsible for the plethora of dissimilar blockchain projects. While a diversity of projects seems to stimulate inclusion and competition, the close look at the actual development of them reveals a false diversification. This misconception at the same time detracts from the main characteristics of the blockchain as a folded apparatus of digital production of control and sovereignty (this is developed in the second part of this chapter), and feeds a blockchain imaginary with dissimilar utopian capacities. An exploration of the role of "decentralization" via Langdon Winner's notion of political design will clarify the significance of the term beyond its immediate discursive use.

Winner argues against the usual idea that it is people's use of technology, and not technology itself, that is political. He understands 'politics' as arrangements of power and authority in human associations that include the design and use of technological devices: "rather than insist that we immediately reduce everything to the interplay of social forces, it suggests that we pay attention to the characteristics of technical objects and the meaning of those characteristics" (Winner 1980, 123). Winner distinguishes two ways, inherent and non-inherent, in which an object can have political properties. In the former (inherent), the system *requires* certain kinds of political relationships that "(...) are strongly, perhaps unavoidably, linked to a particular institutionalized patterns of power and authority. Here, the initial choice about whether or not to adopt something is decisive in regard to its consequences" (Winner 1980, 134). This kind of relation is deliberately designed or strongly compatible with a certain ideology. In the latter (non-inherent), the device design can also be easily adopted by a certain pattern of power or authority or establish a new one. However, this political relationship is circumstantial, as it can be subjected to change depending on the different practical uses of the artefact. Therefore, it does not *require* the maintenance of determined social conditions. Winner's main example is the low

bridges on Long Island in New York, built by Robert Moses, which were designed such that public transport buses could not use them. The argument is based on Moses' alleged discomfort with users of public transit (poor people) reaching his public parks. The main argument of Winner is that it is necessary to look both at the use and the design of technological devices to observe their political qualities. Artefacts like an atomic bomb, a factory or even a ship are, for instance, designed to be ruled in a hierarchical, authoritarian and centralized manner. Regardless of whether or not the process of decision-making around the aptness of these kinds of machines can be sorted out democratically, their technical operations, like the triggering of a device, requires the expression of hierarchical authority.

Blockchains are only 'compatible' with centralization: "a given kind of technology is strongly *compatible with* but does not strictly require, social and political relationships of a particular stripe" (Winner 1980, 130). The distributed ledger of the blockchain does not require centralization any more than decentralization, at least for the technical system to fulfil the basic necessity of genuinely updating the ledger. Blockchain technology, however, remains s*trongly compatible* with centralized systems, and thus it is being implemented privately by different institutions, especially in the financial technology sector. On the other hand, a hypothetical blockchain made of all the world's population, evenly distributed, would not be instrumentally different. Blockchains are thus, equally compatible with centralized or decentralized systems, but all blockchains *require* social and political relationships where the control of trust is displaced from institutional production and recording, to computational production and recording.[13]

The nuanced relations between these terms (distributed and decentralized) and between the notions of public and private, complicates the categorization of the Bitcoin blockchain. I have distinguished these terms to clarify their relevance and association to critically pinpoint the phenomenon of the blockchain. My reading also strengthens my claim that while the groups analysed contest the vacuum of authority left by the open nature of Bitcoin project, neither

13 Matteo Pasquinelli uses the term mathematical recording, when researching the database as a political form (Pasquinelly 2017). I prefer to use the more concise 'computational' term.

of them fully reclaims this empty space; that is, neither provides a convincing legitimation of the system. As previously indicated, my position is that in public blockchains, and specifically in Bitcoin, authority is displaced from external institutional actors to the technical system. The next section of this chapter will analyse this displacement and its association with the technical operation of the blockchain. The operation of mining (or production of tokens) plays a key role in this discussion, as it is to this particular technical performativity where legitimation is outsourced, and from which the system makes itself accountable through computation.

1.2 Automated Anomalous Production

The rest of this chapter offers in the first place a close observation of the production model of the blockchain, and then a theorization of the specific notion of power that is distilled from this model. I refer to it as an anomalous model of production because it consists of an apparently contrasting pair: a token singularity embodied in the form of a digital asset, produced by a distributed infrastructure without ownership. On the one hand, a cooperation-based public infrastructure, on the other, the multiple but unique singularities of digital private property produced by this very infrastructure. The blockchain itself is the folding together of these two deceptively opposed pieces. In fact, one is not without the other: digital private property exists only due to the digital public distribution modelled by the blockchain, and vice versa. Mining, or the mechanism to generate tokens (bitcoins, litecoins, ether, etc.), crystallizes this process, which is at the same time a validation of exchanges, the production of units, and the distribution of information. While it is possible to focus on each separately, they are performed holistically.

I will distinguish between a material and a logical layer of mining to show how the process is at the same time based in and exploiting an idea of superabundance, or unlimited resources. First, I analyse the increasingly evident excess involved in the energy consumption and production of waste of specialized hardware for the double purpose of securely validating transactions and producing tokens. I call this the hardware (material) layer of production. I show how in this layer excessive use of energy is represented in terms of waste and

efficiency. The indication of Bitcoin's inherent materiality paves the way to address deeper layers in the process of production, and allows me to offer a reading of the notion of control in relation to the work done by this process.

Mining I: Waste and Excess

In her recent work, Tiziana Terranova has drawn attention to the necessity of questioning how algorithmically-enabled automation works "in terms of control and monetization" and "what kind of time and energy" gets subsumed by it (Terranova 2014, 387). Cryptocurrencies are payment technologies that automate the production of money-like tokens (Bergstra and Weijland 2014) following algorithmic rules to maintain a fixed production rate. Different kinds of energy and residues, which are not always acknowledged, are involved in this process. The more visible end of the production cycle known as mining shares a definition of waste and energy consumption shared with many electronic devices.

An introductory video to Bitcoin explains that "the bitcoin network is secured by individuals called miners. Miners are rewarded newly generated bitcoins for verifying transactions." (WeUseCoins 2014). Miners are machines that verify the signed public keys for each transaction and which validate these into blocks in a public registry (i.e. the Blockchain). The job for successfully validating and packing the transactions produces new tokens for the miner, and generates a Proof-of-Work. The former is the result of a 'puzzle', which can be then easily checked by any other machine in the network. Since the design of the system seeks a controlled pace, if the coins are generated too fast (because there are more and/or stronger miners) the 'puzzle' becomes harder (Nakamoto 2008b).[14]

Solving puzzles to produce tokens directly translates into a relevant issue of consumption of energy and production of waste. From the deployment of Bitcoin up until the middle of 2010, mining was a task that any modern CPU could handle, even though the process would push it to its limits and heavily reduce its lifetime. Until mid-2011 the workload moved to GPUs, but was rapidly surpassed by FPGAs (Field Programmable Gate Arrays), which reduced energy consumption while

14 I will address relevant details on the functioning of the 'puzzle' in the algorithmic layer section.

achieving more hashes per second. The next natural step were ASIC miners (Application Specific Integrated Circuit) at the beginning of 2013.[15] These iterations are part of a constant evolution in the competing field of mining. The evolution of puzzle-solvers goes from available multi-tasking machines (e.g. any desktop computer) to designs exclusively made for this task. With this evolution also comes a new kind of exclusive waste, generated by swiftly replaced mining boards.

Even though the Bitcoin network was maintained at the beginning by every enthusiast with a computer and some energy to spare, today the mining industry is populated with pools and dedicated farms. This evolution was foreseen in Bitcoin's design (Nakamoto 2008a). In pools, different miners contribute their processing power to calculate a block together. The reward is then distributed among them, usually accordingly to the computational power given, although each pool has its own share protocols. Each one of these clustered miners can have one or multiple ASICs. Mining farms on the other hand are dedicated places that behave in a more or less Fordist fashion, and are even located in old factories or abandoned stores, which house swarms of ASICs (Paul 2015). The energy consumed in farms is striking. A paper from 2015 estimated that the mining network at the time consumed about the same amount of electricity as Ireland (Malone and O'Dwyer 2014). Although mining units energy efficiency has improved in the last years, the difficulty variable has grown too, and the energy footprint problems of production remain. To cite a specific example, one farm operating in 2015 had been told to have 10,000 S3 mining units (Mu 2015). The *Antminer S3* is able to produce 441 Gigahashes per second and consumes 800 Watts per Terahash: that is roughly 4761 Watts in a day, for just one unit. A farm with 10,000 of these units would consume 47,616 Kilowatts a day. Comparing these figures with home energy consuming estimates in the U.S.('How Much Electricity Does an American Home Use? - FAQ - U.S. Energy Information Administration (EIA)' n.d.) shows that just this farm consumes 1,571 times more energy than an average household every day. Mining, today more than ever before, is a race, and reducing the energy footprint is not grounded in pollution awareness, but in cost cutting. As mining units become progressively more energy efficient, they simultaneously become more obsolete. A constant refill of state-of-the-art equipment is necessary to stay competitive. According to Michael Bedford

15 For a history of Bitcoin mining hardware, up until the end of 2013, see Taylor (2013).

Taylor, it took four years to achieve the third generation of mining hardware, and although there are no figures of the number of ASIC units being produced and sold, it would be fair to assume that there is no market comparison with the consumption figures of the smartphones, tablets and other popular devices.

Units by themselves are not more threatening than a colossal mountain of used smartphones, what is menacing is the mono-task logic that produced them. Unlike the smartphone market, mining units do not suffer of a short life because of their hardware resistance, cheap materials or consumption trends; 'planned obsolescence' for ASICs, rather, resides in the scarcity model of Bitcoin's design. Tokens have a fixed limit (21 million) and are getting harder to obtain, so the fast production and consumption cycles of the hardware are intrinsic to the system. At least until the mining becomes unprofitable, in such a scenario, the number of miners diminish and, with it, the difficulty (which, again and recursively, makes the people interested in mining to go up). Difficulty, however, rarely drops, and in the long run describes a stepping curve ('Bitcoin Difficulty Chart - Chart of Mining Difficulty History' 2015), which causes mining hardware to age fast. As specific circuits optimized for hashing, ASICs do not have a second life. Unlike GPUs, they are useless for any other tasks, which makes them completely worthless after their efficient, yet short, life. Since there is no second hand market for mining units, they rapidly contribute to High Tech trashing problems. Electronic waste arguably conforms today about the same amount (in municipal numbers) as plastic packaging waste (Puckett and Smith 2003). Most of the e-waste is recycled in foreign countries because of low labour costs and loose environmental regulations both externally (at least in the U.S. for export of hazardous materials) and internally (waste handling in the host countries). Arguably, around 80% of e-waste is exported to Asia, and 90% of these to China (Puckett and Smith 2003). The hashing power that runs throughout the bitcoin network —i.e. he most and more powerful machine miners — clusters in China too. As of September 28, 2015, on a rough estimate (https://blockchain.info/pools) more than 50% of the hashing power is concentrated in Chinese mining pools and a significant part of the rest is in the U.S., meaning that most of bitcoin's e-waste will eventually end up in Asia.

E-waste is a residual of production that is not reintegrated to capitalist production cycles and thus marks one of the many crises of it, as Jennifer Gabrys argues:

> Remainder breaks with sustained cycles of productions; it moves us past what might be seen as a Marxian concern with the way raw materials are mobilized for production (...) interfering with any notion of a simple feedback loop from production to consumption, remainder calls attention to the after effects and transforms the material arrangements that emerge through the density of our technological and cultural practices (Gabrys 2013, 41).

Mining waste is an immediate leak of its own cycle. Since it has no secondary use, it is discarded faster than less specialized electronics. It is waste that exceeds production. Mining devices of Bitcoin and other cryptocurrencies insert themselves indiscernibly among the electronic waste in scattered dumps, but its particular mono-tasking characteristic makes them suitable non-recyclable remainders. Waste in ASIC units follows the general fate of the discarded microchip industry, escaping the loop cycle and disrupting economies and ecologies at the outskirts of capitalism's production. The number of mines and of ASICs in them is obscure. Nonetheless, as said before, the quantity of e-waste coming directly from mining does not compare to the waste produced by other gadgets. The discussion around excess is not so much framed in quantity, however, but in its lifespan and purpose: hardware mining units are limited to the one and only task of solving the Bitcoin puzzle.

In response to the question of whether Bitcoin mining is a waste of energy, the Bitcoin Foundation answers that: "spending energy to secure and operate a payment system is hardly a waste."('FAQ - Bitcoin' 2015). It is not considered waste as long as the system works. The idea of waste is superseded by efficiency, and annulled in a scenario where the system is fully operative. The substantial empty computational work, energy usage, and e-waste produced in the mining operation has no other goal, and so far no other purpose, than to keep the machine running to produce secure, distributed and artificial scarcity. Within the hardware layer energy is translated into efficiency and residue into excess of

production. The former adaptations happen under a discourse concerned with the maintenance of a secure payment system. However, the hardware uses formerly described are mainly underpinned by the rationale of the algorithmic layer. This preceding layer has, as I will argue, its own notions of excess and a different reintegration into the production system.

Mining II: Superabundance

The efficiency and superior security of the Blockchain system has eventually translated into compelling forms of symbolic and exchange value, as its specific algorithmic value —which I define as the capacity to distribute security in a system via computational power— gained media attention. The exchange value of cryptocurrencies in particular grew as their market performance developed, until its tokens were effectively considered a kind of financial objects. A rush to adopt and exploit the venues followed as the system become prevalent, in great part due to its speculative disposition, which can be exploited as the tokens get exchanged with fiat currencies. Thus, mimicking traditional financial behaviour, like the widely known (Bitcoin) bubbles of 2013 and 2017, or the current wide distribution of blockchain technology in the financial industry.[16] The catalyst for their eventual exchange value is, however, the intrinsic value of the algorithms designed to maintain an artificial scarcity.

Modelled scarcity can be considered through what has been defined as "governance by design," which is "the process of online communities increasingly relying on technology in order to organize themselves through novel governance models (designed *by* the community and *for* the community), whose rules are embedded directly into the underlying technology of the platforms they use to operate" (De Filippi 2015). Bitcoin's communities participate in a designed governance, not only in the sense that rules and development are audited and enhanced through consensus, but in particular because the latter is obtained using the platform (i.e. the branch, fork, and version of the software with a majority of users become the 'de facto' Blockchain). What is more, scarcity is part of the rules enabled by algorithmic governance because, while specificities may be open to

16 A recent example of this are the Initial Coin Offerings (ICO) which, emulating the Initial Public Offerings of the stock market, seek funding by selling tokens to investors.

discussion, the enactment of the rules resides in a purely algorithmic dimension. For example, regarding scarcity, even though the limit of bitcoins is now fixed to 21 million, this figure is potentially subjected to decisions of the community; however, regardless of the total number of coins, the generation of new ones is algorithmically adjusted to sustain production in relation to a ratio of difficulty, blocksize and time between each block generation. The resolution framework and enforcement of rules are hardwired to relational data schemes interwoven by discrete steps of precise instructions.[17]

The puzzle analogy is only appropriate within its algorithmic dimension, which means it must be understood not as a toy or a game, but as a problem that must be solved by following a set of rules. More accurately, the puzzle consists of generating hashes (a string of numbers and letters with a defined length) until one of them fulfils the requirements of the variable 'difficulty' level (in the case of Bitcoin, the number of zeroes at the beginning of the resulting hash). This operation, also called a CISO (Constrained Input Small Output) problem is solved by trial and error[18] and due to the random number involved in the process – the 'nonce value' – finding a 'desirable' final hash is a truly exceptional event (Courtois, Grajek, and Naik 2014). Every attempt to come up with a successful hash uses a new random number, thus randomizing the result. Difficulty is hence, in this context, associated with probability and far from tribulation. Regarding Bitcoin, difficulty is an algorithmic adversity.

The difficulty variable (*D*) at the 19th of September 2015 was set on 59,335,351,233.87, which translates as a 2^25 x *D* number of average hashes to find a block. This means one opportunity to build a block for every 19,909,640,081,173,010,000 (*A*) tried hashes. The only way to deal with the odds involved in this operation is to have a machine capable of generating as many numbers of attempts per second as possible, i.e. an ASIC miner. A state-of-the-art dedicated unit available today can manage to make about 5,500,000,000,000 hashes per second.[19] To calibrate the surplus involved, it is better to think of it in negative terms: unlike the lottery (at which a lonely miner would have better odds) where every non-winner plays a passive role, the miner is a machine that

17 Here I am referring to Berlinski's general definition of algorithm.

18 Alternatives have been suggested to improve this procedure with less costly computation methods (Courtois, Grajek, and Naik 2014).

19 SP20 Jackson by Spondoolies-Tech (http://www.spondoolies-tech.com/products/sp35-yukon-power-shipping-from-stock).

actually uses computational power to actively generate around a sextillion (*A* - 1) useless hashes. I suggest that the algorithmical layer of Bitcoin production is superabundant —underpinned by the idea that digital resources are not bounded — since the mining operation is based in the generation of a sextillion unusable strings.

Designed scarcity is only maintained in a decentralized network via the rules embedded in the excessive use of resources as explained above. In a chapter entitled "Economies of Abundance," Gabrys (2013) describes Robert Noyce's micro-chip sell strategy.[20] This strategy consisted of selling integrated circuits (which were not as popular at the time) for less than their actual cost. This risky strategy paid out by enhancing market value through the necessity for microchips as more machines relied on them. In a way, Noyce not only designed a sales strategy, but the pervasiveness of the microchip. Within Bitcoin, the original design of scarcity in a functional distributed system is also the blueprint for the pervasiveness of excessive computational work.

Bitcoin and other cryptocurrencies are not systems inherently designed for waste nor significant concerns in that sense, and their peculiar mode of production involves a behaviour shared by many algorithmic devices.[21] Yet, they are a telling example of how the idea of unlimited resources gets embedded into automatized and instrumental apparatuses. Ignoring the more obviously material e-waste (Gabrys 2013), the enormous surplus of the algorithmic layer (a continuous sextillion number operation procedure) is underpinned, to some degree, by the idea that digital informational resources, unlike its more overt material counterpart, *can't* be excessive. There is a rationale of unlimited resources attached to the idea of the digital, in part because it is still understood as immaterial. Gabrys reminds us that "waste and waste making include not just the actual rubbish of discarded machines but also the remnant utopic discourses that describe the ascent of computing technologies" (Gabrys 2013, 4). 'Virtuality' as immateriality is a live fossil of the rise of computing and its spread onto popular culture and mainstream use. What is more, rather than eventually becoming

20 Noyce was the manager of Fairchild Semiconductor, and then co-founder of Intel, see Berlin (2005).

21 Much of the cryptography involved in Bitcoin was developed to improve security in different devices, and is used on a day to day basis by generally accepted payment systems (e.g. Europay, Mastercard and Visa) (de Jong, Tkacz, and Velasco González 2015); (DuPont 2014). Also, see Chapter Three of this thesis.

recognised as material due to its entanglements with users, waste, or servers, digital immateriality has not disappeared.

Countable: The Computational Control of Trust

Algorithms have been successfully integrated into the capitalist economy in notorious ways (Gerlitz and Helmond 2013), mostly as a means of production which generates value by monetizing and accumulating social knowledge, from cognitive means to user behaviour (Terranova 2014, 383). Bitcoin is somewhat unique in this sense, since it is heavily driven by the algorithmic production of tokens designed to be themselves a novel kind of exchange value. It is tempting to see Bitcoin and other cryptocurrencies as devices attempting to resist the controlled cycles of capitalism production system, as utopian machines. Automation —human knowledge, skills and work absorbed into machines— can develop productive powers not always contained by capitalist economy (Marx 1980, 696). Nevertheless, I argue that the surplus in the algorithmic layer of production (i.e. the excessive operation of mining's algorithmic layer) is not released from the production cycle —as is the case with e-waste— but reintegrated into it, both by the security design of the device and by the scarcity model as a new means of control for an algorithmically-enabled economy.

My argument follows James Beniger's (1986) seminal work to understand the economy of information as means of control, and Alexander Galloway's study of protocol as a design for decentralized control. Beniger proposes that the industrial revolution generated a crisis of control, when communication technologies and information processes lagged behind the fast developments of energy technologies and their applications (Beniger 1986). The current economy of information is thus seen as a reaction to the accelerated improvements of manufacturing and transportation of the 19th century, what Beniger calls the "societal control revolution" of the 19th and 20th century. In his view, control is the capability of one agent, human or not, to influence another with a determined purpose. Within communication technologies, this purpose is directed to information processing. In a similar fashion, Galloway (2004) updates the discussion on control by considering the specific form that the internet brought.

His work is a critique of the network influenced by Foucault's studies of historical episteme's of power/knowledge. Backed up also by Deleuze's 'Postscript on Control Societies' (Deleuze 1992), Galloway focuses on the internet as an apparatus of the society of control. He identifies protocol as the management style of this new apparatus and defines it as "a set of recommendations and rules that outline specific technical standards" (Galloway 2004, 6). Protocol is able to manage control despite inhabiting a distributed diagram (unlike the centralized or decentralized conditions of sovereign and discipline societies, respectively). Technical devices appear in political life, not only as a direct force of domination, but as dispersed technical devices of a larger apparatus (Foucault 2012). While Galloway acknowledges that the control society and its networks are comparatively more democratic than disciplinary apparatuses, he clarifies that central points of control still exist. More importantly, Galloway argues that current networks, even if made of heterogeneous and fluid materials, are still organised through the systematic management of protocol. By turning bodies into statistical entities through sets of rules intrinsic to the blueprint of the network's system, the management of life as "distributed masses of autonomous agents" (Galloway 2004, 87) becomes possible.

Bitcoin's production system, as Beniger argues about control, is a recoupment of communication over energy. Unlike the residues of the hardware layer that escape the production cycle, the generation of unused hashes of the algorithmic layer are reabsorbed into the system: excessive computation, fuelled by randomness is *a priori* for performance. The continuous generation of hashes – Bitcoin's instantiation of digital superabundance – is a subtle strategy for both the conservation of a state (scarcity) and for the supervision of a decentralized informational system (a secured ledger). Terranova warns that alongside automation new types of control and strategies to reintegrate surplus are also generated, "[automation] must be balanced with new ways of control (that absorb and exhaust) the time and energy thus released" (Terranova 2014, 385). From an algorithm's own logic, the excessive random hashes are not wasted because they are not residue; on the contrary, they remain in the system as enablers of the key states of scarcity and security. In a scenario where Bitcoin's distributed system operates successfully, the algorithmic excess of the system should not be considered waste, but a digital element of control. The use of randomness and the

logic of unlimited resources that comes with mining is protocological: it turns actual energy consumption and superfluous but intensive calculation into a management system.

The pervasiveness of a coded computational mindset is, of course, not exclusive to the blockchain. The integration of randomness through code into a diversity of systems as both a mode of thought and platform for the enactment of its own use and consumption (Parikka 2014) is becoming ordinary. One of my favorite examples, No Man's Sky, is a recent space exploration game that exploits computer-made virtual worlds. While it is not the first game to use 'procedurally generated' elements, the game made use of this technique as a basis and banner for its launch. Most of what exist in the game —star systems' order, flora, fauna, behavioural patterns, etc.— is procedurally generated as such. By giving the game a set of simple rules and variables, the computer generates every possible combination of them. The result is the overwhelming possibility to explore 18 quintillion planets. The creators advertise the factual impossibility of the task as one of the highlights of the game: "if a new planet was discovered every second after the game comes out, it would take 584 billion years to visit every one just for a second" (Hiranand 2015). Outsourcing design labour to the computer, allows the production of large amounts of content with the use of random combination of individual elements. These elements are human-made, but their factual combinations are generated by the computer. The combination of randomness and computer-made operations results in unpredictable outcomes, even for the developers.[22]

In the blockchain, the labour to generate numbers, validate transactions, produce blocks and introduce new tokens into circulation is almost fully automated. The human part of the miner assemblage is free to modify some variables of this process, but has to ultimately adapt to the rules of the protocol (the decision-making of these rules is analysed in Chapter Five). The human miner is a maintainer of their machine counterpart. On the one hand, the design of the system relies on this idea of superabundance, and on the other, the actual algorithmic performance works through its own mode of thought. Bitcoin proof-

22 It is interesting to observe that the promise of infinity was good enough to lure a considerable interest before the release, but the hype among the users faded shortly after. Wide computational permutations in exchange for narrative, was not enough to impress an understandably angered human audience.

of-work is a non-human, non-mechanical kind of labour —“algorithm-made” (Coeckelbergh 2015, 94)—that produces new tokens. Aside from programming and setting up the machines, barely any human labour is involved in the process. Both programming and setting up the machines are not by any means small tasks, and they depend on an assemblage of a huge number of names, discussions, infrastructure, discourses, electricity, investment, and so on. Machines are not built by nature, “they are ‘organs of the human brain, created by the human hand’; the power of knowledge, objectified”(Marx 1980, 706). However, the production process is executed exclusively by algorithms: labour is predominantly digital, what remains instrumental is only the arrangement of labour. What is more, because the nonce value plays a key role in the process, randomness becomes a fundamental for production. Luciana Parisi argues that this randomness is the founding condition of programming and with it our notion of logic as rationality gets surpassed: “this new function of algorithms thus involves not the reduction of data to binary digits, but the ingression of random quantities into computation: a new level of determination that has come to characterize automated modes of organization and control” (Parisi 2013, ix–x). Algorithmic randomness, more than being a systematized reproduction of rules or an applied representation of rationality, works as an outbreak from it, and points to different modes of control. What the blockchain distributes is the control of trust, the confidence that no matter how extended the universe of shareholders, all recorded statements are valid. This consistency has the caveat of being computer-made. It is the big breakthrough of Bitcoin, and all blockchain systems inherit this basic, but crucial operational characteristic. The primordial finding of Bitcoin’s anonymous designer was to solve the Byzantine General’s problem (Lamport, Shostak, and Pease 1982), which requires an algorithmic implementation for secure communication and common agreement among unreliable peers (Nakamoto 2008). The solution of the blockchain means solving the computational puzzle through mining. The operation effectively solves the Byzantine General’s problem by generating a computer-made operational version of trust. This computer-made operation is at the core of blockchain technology.

What No Man’s Sky and blockchains share, among other things, is the predominance of computer-made elements for their operations. In the case of the blockchain, shared trust is displaced from institutions and a diverse array of social

interactions, to the instrumental operation of mining. Specifically, it is the controlled distribution of trust that makes blockchains unique. Blockchains make possible a mode of control that performs even among distributed, fluid, pseudo-anonymous, and apparently non-authoritarian social schemes. Like protocol, they provide a type of control tuned to the pace of decentralized arrangements.

Accountable: The Management of Anomalous Production

Langdon Winner quotes Friedrich Engels' small essay *On Authority* to provide an example of an imaginary situation that does not require hierarchical rule, yet nonetheless is characterized as being an authoritarian system. In this hypothetical instance, land and instruments of labour have become collective and control is apparently decentralized, however, Engels warns that authority —within a cotton mill and industrial environments in general— would pass from a few capitalists to the 'authority of the steam', which is the timed operational work necessary to keep the mill running. Engels adds that "The automatic machinery of a big factory is much more despotic than the small capitalists who employs workers ever have been" (Engels 1978, 731). In this kind of control system, intentionality can be ignored, since authority is embedded in the device, not as addendum, but as a main property. Engel's example is relevant, because it considers that the rules for timed labour are set by the workers in the cotton mill, but once they are put into action, the machinery takes over, leaving little space for autonomy. The same can be applied to the human-made rules that design blockchains, which get surpassed once the system is operational. As explained before, both the ownership of production and control of the registry are computer-made. Particular meanings of control, trust, and authority are folded into the instrumental operation of production and recording of the distributed ledger.

In a recent talk, Armin Nassehi (Nassehi 2017) elaborated on the idea that technologies have created an excess of control, and pointed at an important difference in how we deal with information before and after the dominance of digital communication technologies. In his reading, previous systems validated knowledge by *accountability*. That is, through the authority of the sources. The epistemological soundness of news, for example, was underpinned by the veracity

of the source. The ubiquity of processing of discrete data, or paraphrasing Engels, *the taking over of the machine*, made a significant turn into *countability*. Nassehi argues that now our validation of information is procedural, driven more by the algorithm than by the authority behind it.[23] Matteo Pasquinelli (2017) makes a similar claim and argues that today the statistics feeding the algorithms take control of sensitive decision-making, e.g. US drones autonomously *decide*, based on pattern recognition and anomaly detection, where to strike in a topological data landscape. My claim is that the notion of countability has not really subsided accountability, but that accountability has folded into countability, and that blockchains are an archetypal example of this folding action. In them, the steam machine (the countable) has become legitimate (is *accountable for*). This legitimacy does not come from any external source, but built into the system. With this in mind, I will close this chapter by framing a notion of power that takes into account the algorithmic model of production (mining) previously developed.

Scott Lash (2007) argues that cultural studies must change its conception of power as domination through ideology or discourse. In his reading, both power and resistance have become post-hegemonic. Strongly relying on Foucault, Lash traces the shift from what he calls extensive to intensive politics. He identifies that extensive politics are framed by an epistemological regime, and in them power is enacted as power of one entity *over* another entity, and expressed in terms of *normativity*. While extensive politics are based on the Kantian (Kant 1999) motto of knowing things by its predicates —i.e. not what something *is*, but what are its qualities— intensive politics would in theory replace cognitive judgements with questions of *being*. He also states that power within extensive politics is not enacted through an external determination, but from within. Lash argues that hegemonic power works like a mechanism, through *potestas* (*poivoir*), executing or reacting to an external force. On the other hand, intensive power works more like *potentia (puissance)*, vital force or energy (Negri 1991). Power in this sense unfolds itself from beings. Within this intensive regime, communication replaces the symbolic, which, Lash argues, is the 'iconic of hegemonic power'. Sovereignty and all kinds of legitimate domination with the dual role, of the ruler and the ruled, collapse into the order of communications. Legality is then displaced as legitimation, and replaced by the immediate performance of communications

23 The taking over of accountability by countability seems to be particularly relevant for the discussion of post-truth.

flows. Lash follows here Lyotard's critique of postmodernity (Lyotard 1984) and the association between technology and modern performance as pure optimization. For Lyotard, technical devices "follow a principle, and it is the principle of optimal performance: maximizing output (the information or modifications obtained) and minimizing input (the energy expended in the process). Technology is therefore a game pertaining not to the true, the just, or the beautiful, etc., but to efficiency: a technical 'move' is 'good' when it does better and/or expends less energy than another" (Lyotard 1984, 44). Both Lyotard and Lash recall Luhmann's proposition on how the normativity of law is replaced in post-industrial societies by performativity of the processes (Luhmann 1975). According to Lash, legitimation of previous political systems was made discursively, through serious speech acts, whereas legitimation is intrinsic to communication systems.

An extended theory on how legitimation inherently happens in communications systems can be found in Hardt and Negri's (2001) characterisation of the political order known as Empire. The 'despotic' normativity of the machine, as Engels calls it, becomes in Empire a revolution of the notion of sovereignty previously held by the Monarch and the State. In the transition from monarchy to a democratic system, modernity allowed the maintenance of order and the domination of aspects of the previous apparatus without the necessity of a transcendental entity (as a unity, such as *the* King). A social contract (cf. Hobbes, Locke, Rousseau) made it possible to entrust the powers of the multitude to the figure of the state through norms. According to Hardt and Negri, it is in this period of extensive politics, where capitalism as an economic model was able to flourish and the market was marked as a ground for "the values of social reproduction" (Hardt and Negri 2001, 85). The state in late modernity is reduced to its minimal expression, yet is a necessary element for the preservation of the new system of capitalism and sovereignty. However, as Empire develops, the state is overshadowed by the corporation, especially those related to communication technologies. Corporations not only replace the role of the state regarding the articulation of biopower and global order, but they also restructure this space. They occupy the place of colonialist and imperialist systems, but at the same time deprecate "the imposition of abstract command and the organization of simple theft and unequal exchange" (Hardt and Negri 2001, 31). That is, they do not

behave like states in this sense, yet the state's symbolic power remains as a placeholder, and the state's bureaucratic structure is kept as a tool to record "the flows of the commodities, monies, and population that they set in motion" (Hardt and Negri 2001, 31). As industrial and financial corporations produce commodities and subjectivities (needs, bodies, and social relations), power is enacted by corporations in the process of production, but not expressed as domination between two entities. Instead, power is reflected in the organization of what is being produced: it is in the management of production where the corporation expresses authority. Organization acts as a ghost limb of disciplinary state, which was responsible for the management and distribution of resources, but since legitimation does not come from a centralized institution any more, it is then displaced to the process itself.

However, unlike corporations, public blockchains like Bitcoin lack hard ownership and a defined body, due to their 'open' qualities. Unlike Google, Facebook, Uber, and the majority of strong non-state technology players that behave as a flexible but centralized monopoly, this particular technology is not a corporation, an NGO, a foundation, or any kind of institution. Even the core developers have a small hand in the execution of authority (as is showed in Chapter Five), and are forced to negotiate changes to the protocol with the miners in particular, but also with an extended community of investors, users, markets, and other minor roles. As I have argued, the crucial difference is the headless, yet open, situation that Bitcoin generated. This is more evident in Bitcoin's governance, which makes it an interesting case of study, however, all public blockchains, even if they have more functional and clear authority bodies, lack ownership of the protocol and infrastructure. The mining protocol may differ in their specifics for each blockchain (i.e. Proof-of-Work in Bitcoin [Bitcoin.org 2015], Proof-of-Stake in Litecoin [Litecoin.org 2015], Proof-of-Value in Backfeed [Backfeed.cc 2016], Proof-of-Cooperation in Faircoin [Faircoin.org 2016], but as a basic technique for distributed trust and security —to tame the Byzantine generals — is the blueprint of blockchain technology, and so far shared by all the phenomena of the ecosystem. This impossibility to own the system makes the displacement of legitimation from an organization towards the process of production far more compelling.

A lack of ownership is partly what feeds the dissimilarity of the projects that opened this chapter. The reason lies in the folded production process, which manages to nurture at the same time two different visions of power identified by Foucault. He famously distinguishes two analysis of how power can be characterized, deducted from the economy (Foucault 1980b). On the one hand, he identifies a liberal conception, where power is a right that can be possessed as one possesses other commodities. Because it is subject of property, it can be juridically transferred. On the other hand, he identifies a Marxist conception, where power is understood in terms of its economic functionality, that is, by the role it plays in the maintenance of relations of production and class domination. Foucault does not dismiss the former views, although he does highlight that power in both conceptions is not given and then enacted, but it comes to play in action, as a relation of forces. Power then is performed, and not held.

The political economy of Bitcoin performs both the liberal and Marxist perspectives. First, the big breakthrough of public blockchain technology is the possibility of exchange of value without a centralized authority, that is, the possibility to isolate a system through its own transactions. This allows the arguably flawless transmission of money tokens under a logical infrastructure that cannot be 'possessed', at least not in the same way that a corporation owns its infrastructure. Uber profits from the management of a pure organizational structure, keeping their material assets to a minimum.[24] This lack of assets allows them to monetize the 'sharing' motto in part due to the fact that they don't own any of the products, thus, they can genuinely exploit the alleged sharing culture discourse, playing the role not of owners, but of enablers. On the other hand, for the Bitcoin machine, the assets are privately owned (as much as one can be the proprietary of a piece of data), but the organizational structure, the exchange network, cannot. This does not mean that the behaviour and logic of this structure is not influenced by a socio-technical assemblage, but it does mean that the hard legal property scheme does not apply to it. Then, from a practical point of view, Bitcoin does not rely on legal ownership rights as an authoritative statement, and thus, power as authority is displaced to its fluid productive and transactional properties: the structure is inherently public, the products are inherently private.

24 Also known as SaaS or PaaS, Software or Platform as a Service.

For Hardt and Negri, the most conspicuous characteristic of the complex apparatus of Empire is monetary. In a way, money as a means of circulation is the language of the post-hegemonic apparatus; within Empire, every biopolitical figure is permeated by money (Hardt and Negri 2001). That certainly highlights Bitcoin as a relevant example to be considered within Hardt and Negri's theory. The economic association must be naturally considered, but the crucial element here is that what is produced are fluid digital singularities of private property. This makes its money-like application obvious, but this is due to their private transactional properties, and not some categorization in the economic realm. They are digital tokens enabled to hold their uniqueness (their unique singular status, despite being a digital element), and capable of circulation without reproduction. They *can* be easily thought as money, they are certainly fit for that conception, but it is not an essential relation. This is why blockchains fit the liberal conception of power: as their tokens circulate, they are subject to possession and transaction as commodities.

Regarding the Marxist connotation of power, blockchain technology does little to modify any notion of class domination;[25] if any, it generates new internal subject classes (e.g. the miner) with its own field for domination while, allegedly, depriving the same from other fields (e.g. state banking). However, the system does modify the production of assets.

Hardt and Negri distinguish three paradigms of economic production: agriculture and extraction of raw materials, industry and manufacture of goods, and services and the manipulation of information. They identify that in the informational economy: "the assembly line has been replaced by 'the network' as the organizational model of production" (Hardt and Negri 2001, 295). With network, they refer to a decentralized mode of production for which this networked infrastructure is immanent: information and communication are the very commodities produced " the network itself is the site of both production and circulation" (Hardt and Negri 2001, 298). They state that corporations such as Microsoft, IBM and AT&T were already centralizing massively parts of the information power structure. When Hardt and Negri's work was published, there was no Facebook, Google, or Uber on the horizon. The capitalization of platforms

25 This goes beyond the scope of analysis of this work, but is definitely a relevant matter for future research.

was some years off, but these authors already had identified the dangers and capabilities of corporations to exploit and centralize information, whether by control of infrastructure, or by the concentration of attentive subjectivities and affective production, and generating their own niche kinds of expanding economies (Gerlitz and Helmond 2013). Hardt and Negri use an analogy of the railroad to talk about the immanence of infrastructure, production, and circulation in the information paradigm. Likewise, Bill Maurer (2014) picks up the idea of the railroad system as the 'rails' of money infrastructures to consider contemporary telecom companies as the 'pipes' of the money-token. He argues Bitcoin is a phenomenon where both the token and the *rail* have collapsed into one form of the blockchain.

This folding is another essential characteristic of the blockchain, and the way the means of production is modified. The mining action is at the same time exchange (as accumulation of transactions into blocks) and production (as transactions into blocks are successfully accumulated). This notable process of producing tokens is in a way an implosion of the means of production, insofar as it merges both the instruments (the tools) and the subject (materials) of labour (Marx 1992, chap. 7). The instrument of labor is computing power, while the subject of labor the output of previous computing power. What I have called the anomaly of production is the computational folding of production that merges Foucault's liberal notion of power by generating private tokens (a digital singularity capable of accumulation), and a version of the Marxist notion of power by modifying the relations of production (merging instruments and subjects of labor with exchange, and token generation in a public collaborative infrastructure).

The folding is anomalous insofar as it deceptively feeds an empowerment discourse of collaboration and radical redistribution of power relations. However, I have argued that its main affordance is not to restructure balance in relations of domination, but to grasp a much desired accountability and control in an inherently fluid system. Authority is not distributed among the users or a larger community of stakeholders, but appended to the system in the form of a highly efficient computational management performed through production. This argument also explains the higher compatibility with existing financial systems, already governed by the grammar of statistics, than with co-operative projects.

Open space and the performance of power in the relations of the distributed network do endure, even if they are less visible.

The three clusters attracted by the vaccum of authority disclosed in the first part of the chapter are naturally a generalization of a broader, fine-grained, complex ecosystem. But they illustrate the diversity of projects tucked under the same technological phenomena. They also tell different stories on the ends, substance, and ideals of the blockchain. However, they have very different degrees of existence. Some fade, some are only imagined, others grow sturdily. The promise is in each case propelled by the anomaly in production, which by combining an infrastructural collaborative-based model with the production of digital private property, becomes a flammable material that fuels dissimilar outcomes. The discourse surrounding blockchains exploits this anomaly. The blockchain system is populated with an empowerment discourse, yet its main affordance is far from restructuring balance in relations of domination or modifying the status quo of global financial powers, and closer to tighten accountability and control in an inherently fluid system. Blockchains are a prodigal child of protocol (Galloway 2004). They are a perfect device to provide order over the multitude (Hardt and Negri 2001). Rachel O'Dywer argues that the decentralization of infrastructures does not necessarily correlate with the reduction of the mechanics of domination, as power structures shifts from "dumb-pipes" towards software-based fluid services (O'Dwyer 2012). Blockchains manage to not only to bring back the *bit-pipe* into the discussion by integrating it into the production of software (in the form of mined and secured digital assets), but to maintain a deceivingly adaptable pipe-dream.

Chapter 2: The Political in Digital Methods

This chapter addresses two interwoven notions: first, the methodologies involved throughout the thesis, and second, it narrows a notion of 'the political' that overarches the different methods used. The discussion on the use of 'the political' serves the purpose not only of clarifying the epistemological position of my work, but also as a pathway to stressing the materiality of the blockchain as a socio-technical assemblage accessed through different methodological arrays. Furthermore, the 'political' also highlights the recursive performance of the methods themselves. I understand recursivity not only as Kelty's (2005) notion of "recursive publics" – a group concerned with the technical and legal conditions of possibility enabled by their own association – but also as an action that changes the order of the objects observed, and in doing so, the act of observation. I introduce how this recursivity expresses in the methods used in the following chapters, and acknowledge methodological issues associated with digital methods in particular and in general with the study of computational objects.

2.1 Point of Entry: From Where to Access the Blockchain as a Digital Object?

Blockchain technology presents a methodological challenge due to their multiple readings. Bitcoin in particular, like other digital objects, is not constrained by a single definition. The argumentation I offered in the previous chapter places a reading that stresses these phenomena in relation to how structures and notions of authority are modified by the technical performance and specific affordances of the technological device. However, a field less concerned with the relations between power and technology and more with, for example, the security enhancements that blockchains bring, may offer an entirely dissimilar panorama. Even an observation fixed on Bitcoin can provide a plethora of diverse definitions and narratives of the object, each from a different field. Minimal definitions of Bitcoin been already provided, as diverse as: a digital tool for making payments (de Jong, Tkacz, and Velasco González 2015), a piece of computer software

(Karlstrøm 2014), an informational commodity (Bergstra and Weijland 2014), an egalitarian creation (Boase 2013), or, as Yves Mersch, member of the Executive Board of the European Central Bank, has put it, 'the regional currency of the Internet' (Mersch 2014). It can also be easily defined as a distributed public record, an anonymity tool, and a network of machines. These definitions can agglutinate, overlap, and even contrast with each other, depending on the observing field. Because Bitcoin is at the same time a protocol, a currency, software, a network and a cultural phenomenon, it can play the discontinuous role of instrument, method and object of research.

From the researcher's point of view, Bitcoin is a relatively new digital object. The 'digital' has been defined as 'composed of many different kinds of elements, ranging from computer networks, scanners, algorithms, software and applications to different actors, institutions, regulations and controversies' (Ruppert, Law, and Savage 2013, 31). Many disciplines from the social sciences like media and communication studies, cultural geography, digital anthropology, science and technology studies, internet studies, digital cultures and digital sociology (Wynn 2009) are heavily involved with digital research and some have even been spawned by it (Lupton 2014, 13). However, as technology surrounds most of our activities, a similar fate of the online-offline division occurs to the digital and non-digital distinction (Berry 2014). Information can be produced, mediated, organized or made digitally available in different degrees, this complicates delineating the fuzzy borders between the digital and the social or between the digital and its counterparts (Cramer 2013). Digital and non-digital entities can take the form of native – forms and materials "born" in, and not migrated to a digital medium (Rogers 2013) – and non-native data, subjectivities, techniques, objects, institutions, methodologies, and so on.

Bitcoin, as a digital object, is framed by its own medium-specific constrains and regimes, and also produces its own kind of data, categories and agencies. Due to its novelty, it stands on a challenging starting position. It was designed to be an oxymoron to close observation: regarding its actual technical functioning, it is transparent and public (certainly not without complexities, since its guts require at least a little notion of how cryptology strategies are enabled in software). Observation for this side of the object is open and the working and results for every transaction made with the device are easily available ('Bitcoin

Block Explorer - Blockchain.Info' 2015). Some social aspects of its use are, however, on a nicely crafted dark side. Unlike more traditional research on social networks like Twitter or Facebook, where social content, data and metadata of how these software-enabled platforms are used is gathered and analysed in closed spaces, or even partially available for the non-corporate researcher, the data on cryptocurrencies is democratically scarce. The issues of accessibility are not only in the order of availability of information: the phenomena also posits a general challenge on from which point of view, among the many fields and associated methodologies, should it be accessed.

A creative fiction book by Milorad Pavić, the Kazahar Dictionary, tells different stories in an encyclopedic form. The narrative gets broken or superimposed by the order in which the reader access the text. In fact made of three dictionaries (Christian, Muslim, and Jewish), the same entry may be repeated in each of them, sometimes telling a different story, and sometimes complementing a coherent narrative. The text is challenging and open from the very start, since every entry acts, very much like the name suggests, as a legitimate point of beginning. The path that comes after is not defined either, one can search for the same entry in the other dictionaries, go to one of the suggested hyperlinks to other entries, or even pick a new random word to continue. The form of the text is made so that a narrative is created in the process of accessing it. There is no right point of access or pathway, and order emerges only insofar as the act of reading is taking place. The book exploits this form to delightfully generate an unfamiliar and unprescribed passage.

I am not suggesting that this playful lack of (previously determined) order is a methodological technique to be extrapolated to social sciences research. The entertaining reading of this fictional dictionary, despite any analogy, is not equivalent to academic research of a technological device. However, it is true that blockchains are a good example, and certainly not the only one, of research objects that have different readings depending on the point of entry or the path of inquiries chosen to observe them. What is more, the question on how to access a research object is methodologically relevant. Moor and Uprichard (2014) underline the materiality of the method itself when accessing a complex research object, taking the Mass Observation Archive (MOA) as a case study. The MOA, a database of the everyday life in Britain, is a project based on a nonsystematic

design of samples coming out of self-motivated participation: “The 'Observers' do not constitute a statistically representative sample of the population but can be seen as reporters or “citizen journalists” who provide a window on their world.” (massobs.org.uk 2015). The project has been ongoing since the beginning of the eighties (with a first iteration from 1937 to 1950). While the majority of the archive consists of writings from the observers, it also gathers other kinds of data, such as recorded interviews. Moor and Uprichard highlight the materiality not only of the archive, but also of the act of “getting dirty” with data that the researcher accessing the archive makes. Since there is no digital version of the archive, the researching is confronted with a number of boxes to be opened and explored. Moor and Uprichard stress that even thought the data is there, the way to access it has material consequences: “We cannot get around this problem, regardless of what kind of data we are accessing, whatever the research, whichever methods are used, problems of access are intrinsic to empirical social research” (Moor and Uprichard 2014, 36).

Digital phenomena may appear to have fewer constraints of access and fewer issues related to materiality due to its virtual format. Given its mathematical enclosure and software-based boxes, a notion of neutral access is commonly associated with the digital landscape. An extreme of this deterministic position, can be found in Kevin Kelly’s descriptions of technology. For Kelly (2011), technology offers a degree of objectivity that even allows for a level of agency independent from the human interactions with it. He sees technology not as a set of particular objects, but as a whole; a large “out of control” autonomous being. He proposes the use of the term “technium”, arguing that both “technology” and “culture” fail to describe this entity: technium includes “culture, art, social institutions, and intellectual creations of all types. It includes intangibles like software, law, and philosophical concepts. And most important, it includes the impulses of our inventions to encourage more tool making, more technology invention and more self-enhancing connections” (Kelly 2011, 11). In Kelly’s view the technium is starting to exercise autonomy. For autonomy, he specifically refers to an enhancing of the self in many areas (except self-consciousness, for which Kelly believes has not happened “at this point”): self-repair, self-defence, self-maintenance, self-control, self-improvement. While he acknowledges that there is no single example of technological device holding all the former characteristics, he argues that there are particular examples that perform one or the other. Since his

reading of technology is holistic, and refers to a planetary system, he argues that the technium, as a whole, has a sort of agency. Not only does it want what humans design and command it to do, but also its possesses its own drives.

Kelly's view is controversial: technology is neither completely independent, nor autonomous. It is built by specific humans, travels in specific cables, executes specific algorithms (even if more and more fed by randomness and blackboxed [cf. deep learning, google's AI encrypted language]), and its growth and failures are moulded by chance and the bureaucracy surrounding it (Latour 1996). Hence, while the complexity of the object allows for multiple readings and points of entry, I don't understand blockchains as utterly relativist objects, neither as independent objects such as Kelly's technium.

Instead, my research point of view benefits from the Science and Technology Studies (STS) tradition that understands objects as nodes with its own agency and social weight within networked assemblages (Latour 2007a). This position allows me to anchor my perspective of the object in a middle point in between a technological determinism and social constructivism. While my position is closer to the latter, I do not consider blockchains as a completely designed object, and allow room to discuss a mode of thought befitting to the machine/algorithm and alien to social phenomena (see the notions of randomness and superabundance discussed in Chapter One), but never independent of a network of relations. While the Latourian approach is based on relations between asymmetrical actants, it does not have claims of an overall objectivity. It is closer to the specific objectivity of Donna Haraway's (1988) situated knowledges, which distances from transcendental claims of the individual, objective, neutral and rational observer (Code 2014) —such as Kelly's Technium— and upholds a specific-embodiment objectivity. For Haraway, situated knowledges are about communities made of active meaning-generating material-semiotic actors part of a dynamic apparatus.

However, this research should not be considered a contribution to STS or Actor Network Theory (ANT), since my main interest is not to focus on identifying relevant relations in a network of humans and non-humans. Alternatively, this work is a close analysis of the machine logic of production and the behaviour of its network, closer to the field of Software Studies; a historical dissection of the technologies that preceded it, closer to the field of Media Archaeology; and an

observation of some internal discussion of governance, closer to a digital ethnography. I will elaborate on how the chapters of this study relate to these fields in a moment, but I want to stress that while this work is not an explicit heir of ANT, it does share the particular ontology of partial, locatable objects made *in* their relations, and the epistemological concerns of such ontological stance.

2.2 The Political as Gathering

One of the challenges is how to makes sense of "the political" in such, if not relativist, "relationist" ontology. The fading of archetypal figures of authority and performance of political exercise, such as the state, in digital phenomena like blockchains highlight the relevance of this inquiry. It is not contested that states have strengthened their role in controlling the "free" internet of the 90s, using different techniques such as censorship and division of platforms according to territorial constrains (i.e. China's firewall and their main internet services ecosystem, such a Baidu and Alibaba, as developed in Chapter Four). However, on the one hand their central role as control points is diplomatically contested by transnational corporations; on the other hand, alternative illegal services that also challenge their manoeuvrability keep surfacing from the deep ends of the web. Bitcoin, for example, is in a middle point here: its markets do follow regulation as any other service depending on the territorial law of each country, but at the same time is the *de facto* currency of black markets in the dark web. What I want to stress is that phenomena such as blockchain technology provide an interesting standpoint to reflect on a post-state notion of "the political".

Hardt and Negri point out the transformation of this notion in the figure of the Empire discussed in the first chapter. According to them, the political as 'determination of consensus' or 'sphere of mediation among conflictive social forces' has disappeared. Consensus is now determined by economic factors (e.g. speculation of currencies): "Government and politics come to be completely integrated into the system of transnational command. Controls are articulated through a series of international bodies and functions (...) Politics does not disappear, what disappears is any notion of the autonomy of the political" (Hardt and Negri 2001, 307). This reading considers that in a period of global capitalism,

systematic relationships of transnational corporations and other bodies disperse the *place* of politics. Representation in post-hegemonic times "leaks out", and the ubiquity of computation and media "bequeaths to us ubiquitous politics" (Lash 2007, 71). The identification of the political as a central power is dismissed, and instead it spreads across an untraceable number of actors and relations. Since a delimited sphere of "the political" disappears, ANT as a relational method stance, and its notion of politics, become particularly relevant to rephrase politics.

Latour defends ANT notion of politics in a reply to a Gerard de Vries critique (de Vries 2007). De Vries argues that ANT does not engage with a political position, and suggest that it would benefit from considering existing political philosophies (in de Vries example, using Aristotle as political framework). Latour's reply defends STS exclusion of pre-determined political theories, not because they cannot be applied to an understanding of the politics involved in a relational research, but because they prescribe issues that frame what is to be known of a network. Instead, ANT follows the issues that are generated by the relationships, and previous to the interactions of the network. Moreover, he defends that this research technique does not imply a lack of politics, but a different, perhaps more raw, notion of them. Latour's reading of STS ignores canonical elements of political theories, like 'traditional characters' (citizens, ideologies), 'traditional sites' (demonstrations, control rooms), 'traditional passions' (indignation, anger), "but pays attention to new means through which politics are carried out" (Latour 2007b, 3). Latour ANT's approach is concerned with understanding politics neither as a domain or procedure, nor as a set of beliefs that can simply applied to any situation. Instead, he argues that situations produce their own politics. Latour argues that STS has expanded the vision from the traditional political scientists, by introducing a notion of politics as the composition of the shared world or cosmos (Stengers 2010). Politics in this reading are then issue based (Marres 2007) and generate their own publics, and not a sort of definition to put into use in the absence of any issue. He identifies layered ways in which politics can turn around issues or "successive moments in the trajectory of an issue" (Latour 2007b, 2). First, how a connection of humans and non-humans (neither symbolic nor naturalistic causalities [Latour 2007a]) redefine the cosmogram; then, the moment an issue generates a concerned public; followed by the moment a governmental machinery that turns the issue into a common problem; fourth, the issue gets

absorbed by democratic processes; and finally, it is integrated into bureaucracy. Latuour argues for the relevance of STS in detecting the 'political-1' moment, where "every non-human entity brought into connection with humans modifies the collective and forces everyone to redefine all the various cosmograms" (Latour 2007b, 5).

While my research does not claim to follow or be based on the Science and Technology Studies (STS) tradition, the work on this thesis coincides with Latour's STS positioning: First, I understand 'the political' in a broad sense, and acknowledge that different instances, or moments, can be considered part of the political but researched by different methodologies and theories. And second, I pay particular attention to the early stages of the previously presented *trajectory*, that is, to the way new relations between humans and non-humans (cryptography, developers, mining stations, borders) are put into play in a still undetermined way, and considered these as political relations. Thus, the focus of this study should be considered political in part because it does rely on a political theory framework (it makes use of political economy discussions, e.g. Hardt and Negri's Empire, to discuss the notions of regulation and production and the significance of its outsourcing to computational processes, as introduced in the first chapter), but also because the emergence of blockchain objects reconfigures a network of asymmetric elements.[26] The miner machines, for example, are non-human actors that come into play with other already existing human and non-human actors (like developers, or open source standards), and in doing so, disturb or event create new power assemblages. While this research is not ANT committed, it does share its characterization of power not as reservoir, but as a product of these relations (in the specific case, the relations at play in the production of tokens by distributed computation).[27] The point of view of ANT also benefits the approach to the agency of non-human elements. The computation involved in superabundance and production of authority, as seen on Chapter One, by a bitcoin's mining has no agency by itself. But it does have it in a relational scheme. While not being completely designed, nor self-governed, it becomes a "matter of concern" (Latour 2007a, 114), which is capable of agency when considering as *gathering*, rather than as *object*. While along this work I will constantly refer to blockchains,

26 For Actor Network Theory (ANT), the symmetry does not imply an identity of substances, but to ignore any a apriori distinction between "human intentional action and a material world of causal relations" (Latour 2007a, 76)

27 See Latour (2007a, 71).

cryptocurrencies, and bitcoin as digital objects, I am understanding them with the aid of ANT, that is, neither isolated agencies nor anthropologically designed machines, but as gatherings.

2.3 Digital Methods and Recursivity

Going back to Moor and Uprichard's assessments of empirical research, while digital research may promise easier points of access and stroll through its mathematically-defined categories, these software boxes come with their own methodological challenges. While an ANT stance eases the transition on how to think about the political in distributed digitally-enabled arrangements, the pervasiveness of the gatherings, however, may be also recursive. I will explain what I mean by recursive and how I identify it as a persistent problem in digital methods and digital objects research. Methodologically, each of my following chapters deals with a more pronounced issue of recursivity: cultural, epistemological, and performative. However, all share the main claim that a grammar of digital communications is pervasive in culture and knowledge. Not only because we are used to a daily interaction with digital objects, but particularly, because a computational mode of thought consumes the very way we encounter these and other objects. While this is an interesting subject to discuss at length from, for example, an ethical perspective, my interests here are to acknowledge and question how digital methods in my own work imply a digital mode of thought in accessing research objects.

Cultural Transcodings

The methodology of chapter three (*A techno-political prehistory of the Blockchain*) can be read along the lines of media archaeology. It tracks the lineage of the blockchain components, since the early seventies up until right before the emergence of Bitcoin in 2008. The chapter is an attempt to understand the parallelism of cryptography and money, by also supplying the political context of some of the main pieces that make blockchain technology possible. While Chapter

Three acts as a brief history of cryptography and digital cash, the intention is to provide an explanation, not only of the lineage of the Bitcoin's previous life, but also to explain the actual relevance of a device such as the blockchain by way of exploring the history of its elements. I consider this chapter belongs to the media archaeology tradition, because like it, the method is epistemological as much as it addresses the temporality of the objects. The question of 'where to start' observing an object is what makes media archaeology notable. The archaeologist avoids the figure of the historian, which starts from the beginning, and of the 'analyst' who focuses on current developments of the object of study, and positions him or herself in the middle of these ends. The field builds on the Foucauldian tradition (Foucault 1982) that excavates the 'conditions of existence'. Jussi Parikka summarizes the meaning of archaeology in the work of Foucault: "Archaeology here means digging into the background reasons why a certain object, statement, discourse of, for instance, in our case, media apparatus or use habit is able to be born and be picked up and sustain itself in a cultural situation" (Parikka 2012, 6). Friedrich Kittler expands this Foucauldian approach by adding that this excavation is not restricted to the discursive and institutional realms, but also to media networks and scientific discoveries. Indeed, the discourse associated with blockchain objects is not detached from its own materiality. Kittler stresses that even manifestations of media that lack physical attributes are dependent on an array of machines, cables, routers and many layers of hardware for their performance (Kittler and Metteer 1992). Chapter Three ties a level of discourse with the material cryptography in which this discourse was expressed.

Blockchains are not traditionally understood as cultural media such as cinema or photography, but they can be archaeology tracked as one of the most important mediums of exchange of new media. I identify blockchain technology as a medium, in part due to the circulation properties that their embodiment as cryptocurrencies entails, but also due to my theoretical framework informed by Media Theory. Representation of cryptocurrencies as digital money stresses its distinctive circulating properties, it attaches a digital trail to the notion of money as a medium of abstracted ownership (Krämer 2015). The constitutive transitive qualities of Bitcoin, for example, defined by its author as peer-to-peer electronic cash (Nakamoto 2008b), bestow the intention of using the system as a medium resembling digital money. More importantly, my reading follows the

aforementioned lineage of a foucauldian approach that observes technology as a cohesive element for the operation of power relations (Foucault 2012). Technological objects in this reading are part of authoritative arrangements to control and manipulate groups and individuals. Likewise, my approach follows an observation of technology and media invested in identifying the power configurations that are enacted by the materiality properties media. The discussion on the power, technology, and materiality axis is advanced by a Media Theory approach, which strengthens the role of old and new media in this literature tradition. Thus, my position identifies blockchains, and Bitcoin in particular, as a medium within this line of inquiries. That is, a material technology that performs and is performed within an arrangement of diverse objects and subjectivities, and whose observation as new media is revealing for contemporary socio-technical studies.

Blockchains certainly fulfil Lev Manovich's principles of new media (Manovich 2001, 27). He identifies five characteristics of new media objects:

1. Numerical representation: new media objects can be formally described and subject to algorithmic manipulation.

2. Modularity: media as collections of discrete data.

3. Automation: principles 1 and 2 allow for automation of operations: "human intentionality can be removed from the creative process, at least in part" (Manovich 2001, 32).

4. Variablity is also allowed by the first two material principles: new media objects are not fixed, they can exist in "different, potentially infinite versions"(Manovich 2001, 36).

5. Transcoding: this characteristic refers to the ability of new media to traduce between two layers, a "cultural" (contents, meaning, formal qualities) and a "computational" (file size, compression, format).

The first characteristic, the numerical representation of media, is applied to blockchains without much controversy, inasmuch as they are natively numerical. The information represents may represent different kinds of values (i.e. digital assets), but its primitive form is that of the number. The cryptographic techniques at the heart of the blockchain as medium are an instantiation of numerical and algorithmic manipulation. They also comply with being modular structures of data:

the tokens and validation that takes place in the blockchain conduction are discrete and stackable pieces of information. However, the characteristic of "variability" is not as easily applied. Indeed, the blockchain has a replicable structure. In fact part of its most notable attributes is that of being a distributed database. The information is shared between any number of computers in the network, but unlike the pieces of a jpeg-encoded photography, on the blockchain only part of the information is replicable (the public key), while another is kept private (the private key). This clever use of cryptographic pairs makes each token (i.e. each bitcoin unit or sub-unit) digitally unique, and thus not subject of counterfeit. I have previously (Chapter One) discussed that in the production process of the Blockchain, the accountability provided by the notions of authority and legitimacy is outsourced to computational power. Modularity is relevant here, because as I mentioned, a part of the blockchain is spread and replicated (the ledger and the transactions), while other is unique and non-repeatable (the tokens as digital signatures). Then, how the variability principle works in blockchains must be considered with a pinch of salt. Dissimilar outcomes may come depending on what is looked: a string of a hash, the private key of a transaction, the information acknowledged between nodes, the code belonging to a software wallet, or the code for the protocol version have different degrees of variability. Finally, I am particularly interested in the transcoding capacity of digital objects like Bitcoin. According to Manovich, the transcoding process allows for the substitution of former cultural categories and concepts for new ones deriving from computational ontologies, epistemologies, and pragmatics.

An omnipresent example of new media is the database, which is the form behind many of the interfaces we encounter in the digital. For Manovich, the database takes the form of the privileged narrative after the cinema, which in turn replaced the novel. He defines a database as a structured collection of data, but highlights that this structure, as the combination of data structures and algorithms, depicts an ontology of the world in computational terms. New media objects are interfaces to a database, thus narrative and database do not share the exact same status: "More precisely, a database can support narrative but there is nothing in the logic of the medium itself that would foster its generation" (Manovich 2001, 228). Manovich previously states that databases represent the world as unordered lists of items, while a narrative is the opposite: "a cause-and-effect trajectory of seemingly unordered items (events)" (Manovich 2001, 225).

The blockchain can be read as an interface to a new iteration of the database, and the whole notion of the blockchain fuels the narrative of decentralization through technology. The database in this case is not only an efficient backend for organizing information, but an actual transcoding of notions such as trust and authority into mathematical, statistical, and numerical forms. The archaeology method of Chapter Three recognizes the evolution of this transcoding.

Epistemological Grammar

The use of computational forms in my own research is more evidently shown in Chapter Four, which gathers data from the Bitcoin network to trace a geographical blueprint. While the weight of the argumentation in that chapter is to question which notion of decentralization with empirical evidence and to reflect on which kind of territoriality shapes and is shaped by such distributed networks, these discussions are underpinned by the empirical method used to form the map. I use a small server and a script to gather data from an API of the network, from which I select the most persistent geographical data points (nodes) during six months (I discuss the technical specificities of this digital method along the chapter). The different steps of this digital method are already soaked in a computational ontology. First, API calls offer a limit set of *a priori* formatted categories and definitions for the possible data. The characteristics of the node object exist within this logic. The category of “protocol version” exists as part of the API parameters because it is a relevant piece of information for the effective functioning of the network, while the political stance of the node owner or the general incentives for keeping this node running are not machine-relevant, and thus not available as part of what can be digitally gathered. Traditionally important categories for social research may not appear, in part because this device was not designed for this kind of information retrieval, but also because social categories are not part of most technical grammars. Then, scrapping data from the bitcoin network involves 'medium-specific' limitations, 'alien' analytics assumptions to social research, and an inherent risk of importing 'inquiry categories' into our own (Marres and Weltevrede 2013). The same applies to the distillation process (i.e. the selection of nodes by their persistence, measured by timestamps), also

produced by code categories. While coding in general has broad and creative outcomes, it is also “the manifestation of a system of thought —an expression on how the world can be captured, represented, processed and modelled computationally with the outcome subsequently of doing work in the world” (Kitchin and Dodge 2011, 26).

Philip Agre names this systematic representations of organizational activities in computation as “grammars of action” (Agre 1994). The representation follows what he calls the “capture model” of privacy, which has the deliberate intention of reorganizing industrial work activities to ease computers capturing of tracking information. He pays special attention to the use of linguistic metaphors as one of the attributes of these representational schemes. Agre observes that human activities can be framed as the sum of a set of unitary actions and the rules to compound these activities into sequences. This is what he calls grammar, which refers not so much to the content of each activity, but to the architecture that allows human activities to be represented by computers. The representation of information (the grammar), the intentions that guide the creation of the frameworks used with this grammar (the development), and the multiplication of methods in future epistemological directives, are already embedded in the many manifestations of the digital objects. Both the device (the server, acting as a node), the instructions for retrieval and distillation (the scripts), and the data (the information for each node and snapshot) are considered 'natively digital' (Rogers 2009). This means it is subject of predefined categories, specificities, definitions and interactions that are implicit and may not even be evident. That is, an unavoidable computational ontology comes with the use many digital objects, with its own rules, logic and grammar. The researcher working with digital methods is forced, by platforms and 'medium-specific' inheritances, to become an analyser and a distiller: data collection becomes extraction, and making of knowledge, distillation (Marres and Weltevrede 2013). What I want to stress here is that the very use of digital methods by digital research reinforces in many cases the cultural transcoding previously discussed. Not only on a cultural level, as the use of terms like “data” as information, but also to an epistemological degree: the very same tools and language used to know and make sense of this digital object come from a computational ontology. This does not imply a one way influence: in many cases computational terms and techniques are inherited from other fields,

methodologies and modes of thought. The direction of influence may change. This is what I refer to with recursivity: the use of digital methods to observe digital objects in many cases reinforces a computational way of understanding those objects.

Digital methods are easily transformed into epistemological data; it has been argued that what defines the digital is not its new technical possibilities, but the actual transmutation and multiplication of methods (Mackenzie and McNally 2013). According to this idea, digital methods do not only display data about something in the world, but turn this production into data about how things are known, data that can get dissolved into other digital devices. Multiplied methods become data themselves. The former methodology description shows more about what we are allowed to apprehend via our own methods than about how exactly are machines distributed in the world. Even though it does show the latter, from a methodological point of view the importance of the mapping resides in the epistemological highlighting of relations, i.e. what the location of machines says about how a broader ecosystem is understood. The very process of localization builds up on what we think we can know of this ecosystem. Methods relying on data manipulation replicate this grammar and, in doing so, influence potential epistemologies for future objects. Material logistics involved in digital research methods are not "outside" of data, but ontologically and epistemologically intrinsic to it (Moor and Uprichard 2014). Digitalization requires the researcher to take into consideration the content of the digital as much as the form it takes. This recursivity also expresses in the decision-making of the objects, what I previously refer to as performativity.

Performative Design

Paul Dourish (2014) extends Manovich's line of research of the database, focusing more on its characteristics as an infrastructure, and less as media. Like Manovich, he stresses the materiality of information in this format, and considers it a foundational characteristic of the digital. For Dourish, the digital is *inherently* material, and this materiality is not simply because the structure is represented as electrical or magnetic traces, that is, not only due to its physical infrastructure. It is

also because the material “constraints” allow the specific infrastructure to work in the form of a database, that is, how information is coded for specific executions. In his analysis of the database, Dourish also identifies a relation between the organizations behind the design of data structures and the organizations interests in charge of the development. He argues that the development of System R, a relational data model that was the blueprint of many contemporary database systems, was an overall design not only related with data structures, but with a model to offer computing services and computing architecture manufacturing. System R was developed by IBM, a software provider, a hardware developer, and a provider of bureau services. Dourish argues that IBM’s position allowed the corporation “to develop its computer architectures to enhance performance in executing relational database transactions, and to define the benchmarks and measures by which database systems would be evaluated” (Dourish 2014, 15). The grammar of the relational database in this case, is related to sociomaterial configurations that involve a business model, software systems, and physical manufacturing of an organization. Indeed, the capture process identified by Agre is never completely technical, and it includes elements of interpretation, strategy and institutional dynamics: “capture is never purely technical but always *sociotechnical* in nature. If a computer system ‘works’ then what is working is a larger sociopolitical structure, not just a technical system (…) if the capture process is guided by some notion of the ‘discovery’ of a pre-existing grammar, then this notion and its functioning should be understood in political terms as an ideology” (Agre 1994, 748).

System design marks the third recursivity issue, expressed in Chapter Five. This chapter follows an elongated controversy within the development of Bitcoin. The intention to pursue a governance system ruled by an open model, but with a community with evident dissimilar interests broke the blockchain into at least two opposed kinds of organization with different models and ends. While the decision-making process intended to follow strict rules based on the meritocracy of the code, along with well-designed rules to advance and implement a proposal, the search for an objective governance failed and ultimately showed how technical design is tied with political ends. The chapter shows how the size of a block for the blockchain, a technically superfluous problem in terms of design, is not minor as it is connected to conflicting ontologies. Permutations within digital grammar are

not neutral. They are created with deliberated intentions and goals. Digital transactional data and algorithms are not usually designed with the purposes of social researchers in mind. Although some cases are inherited from academic logics [e.g. Page rank and citation schemes (Beer 2012)] the mould cases for data allocation are made to and from quite different perspectives. At this point Facebook data scientists have access to what is probably the largest concentration in history of social interaction data and metadata (contents, actors, relations), and while their methodological behaviour can resemble that of the social researcher, their ends and aims are most certainly focused into another chain of intentions, and enframed by specific systems of though, political economies and politics (Kitchin 2014). For example, providing a better experience for the user to enhance their business, in order to improve its marketing performance or even create new products (Gerlitz and Helmond 2013; Cusumano, Goeldi, and Dutton 2013), like the Facebook's Messenger or Twitter's Periscope. Similar sets of digital techniques and tools for research are used with dissimilar intentions. What I am stressing here is that a factor of intentionality exists in the development of technology, but also in the methods to understand the technology and the social arrangements involved with it.

This chapter addressed the challenges and complexities associated with my research of blockchains as digital objects. I started by suggesting that the technology is a particular object of research, and offers a multiplicity of points of access, which make relevant the question of from where is it possible to think about its political properties. My position on this is to understand the object with the aid of an STS point of view, that is, not as an independent entity and thus, not located in a technological deterministic position, but as a gathering of relations. This point of view seems adequate for a system that distributes authority throughout a sociotechnical assemblage. Also, the STS position stresses the materiality of digital objects, and the possibility of non-human relations that allow modes of thought closer to computation, and not only as a social construction. I then focused on the general methodological issue of digital methods that is the recursive reinforcement of a computational grammar. That is, the use of a set of categories, that are themselves part of a computational ontology, to understand computational objects. While this issue is not a problem by itself, I consider the

importance of recognizing its recursive status, and that the use of digital methods as tools of research does not only change their *prosthetic* or *instrumental* role (Bradley 2011), but also an ontological one. This recursivity is expressed iteratively in the grammar, the methods, the epistemology and the cultural transcoding that takes place while observing digital objects.

As with many new digital objects, the emergence of Bitcoin generates an opportunity to produce new methodologies. Specific research paths can emerge from what the affordances of novel digital objects bring up, and re-distribute among other social science research methodologies, obeying the argued distributed nature of social research in online environments (Marres 2012). Agencies modeled by digital methods, like 'nodes' on the bitcoin network, inherit attributes from the digital logic of its digital devices, in most of the cases, unavoidably. Then, digital research must consider the implicit contract of working with entities derived from computational sources, specially when tied to extraction and distillation techniques.

An open question is posed by Law and Ruppert (2013) on how dynamics of methods that are shaped by the social[28], that work to format the social, and that are used opportunistically, intersect with each other. Far from attempting to answer such an elusive interrogation, I would add to it that the awareness of current computational ontologies and an acknowledged intention of the researcher to restructure the social, are key to identify the opportunistic shaping of society: how devices collect, communicate and store data, how its grammar belongs inevitably to social and political institutions, and how their usage directly reinforces a kind of knowledge articulated by the devices' own logic. Then, methods should be used and designed considering the former and highlight aspects of the device that are less constrained by computational ontologies. This follows the suggestive path of 'emergent' methods, i.e. inventive methods that "are able to grasp the here and now in terms of somewhere else, and in doing so – if they can also change the problem, to which they are addressed – they expand the actual, inventively" (Lury and Wakeford 2012a, 13); and of 'affirmative' approaches to 'biased' digital research, i.e. methods to exploit the ambiguity of digital devices, treating them as an empirical resource positively marked by bias

28 E.g. Mckenzie (2012) shows how databases' elemental names —*tuple*, *key*, *relation*, etc— were taken from set theory semantics.

(Marres 2015) methods. From this perspective, 'emergence' denotes not only the notion of coming forth, but emerging as a change in the previous state of affairs caused by the devising, use and deployment of methods.

Chapter 3: A techno-political Prehistory of the Blockchain

This chapter is concerned with the origin of Bitcoin. Borrowing a Tung-Hui Hu (Hu 2016) approach, it can be read as a *prehistory* of the Blockchain. Hu shows how the modern notion of the 'cloud' not only grew from older networks but remains layered over them. He also traces the growth of the cloud as an idea that expanded beyond a technological platform. While the blockchain has a relatively young history, both as technology and as a metaphor, this chapter dissects the technical pieces (or "gears") of Bitcoin as the first working blockchain. In similar fashion to Hu's work, this chapter provides a political context from which to understand the function of the Blockchain's gears and also the surrounding conditions that enabled the generation of these gears.

I follow his notion of prehistory in the foucauldian tradition, as a way to provide an understanding of the technical conditions and entities that shape the conditions of possibility for new technology. Hu underlines both the underpinning of new technologies in previous infrastructures, but also how ideas on new technologies portray a powerful metaphors that go beyond the platform as technology to pervade how society organizes and understands itself. My work on this chapter uses this dual notion of prehistory to shed light on two aspects involved in the history of blockchains: first, the political context where its technical pieces materialized, that is, the historical conditions involved in the creation of its structure. I use the term "gear" to refer to the technical pieces or iterations that either are directly used in the software or protocol (e.g. the ECDS algorithm, an iteration based on the RSA algorithm; both implementations of asymmetric cryptography of digital signatures), or that are an implementation of a previously projected technical piece (e.g. Hal Finney's RPoW which inspired the PoW used in Bitcoin). Second, to indicate how these technical pieces gradually entwine with an ideology that pervives not only in Bitcoin, but in subsequent implementations of the technology. Very much like the cloud, 'the blockchain' is also a metaphor that exceeds its technical capacity and materiality. It is a current *cultural fantasy* (Hu 2016, xxiv), partially embedded in the political context of its own technical pieces.

The prehistory of its gears, thus, informs its material constitution and the ideologies associated with its current embodiments.

This prehistory is not exhaustive. It is focused on making sense of Bitcoin as a cryptographic device; one to which a specific transactional value is attributed, which detaches its production and circulation processes from traditional authority institutions (state and central banks). I identify three historical trajectories that interweave with the emergence of Bitcoin: one concerned mostly with secure communications; a second that adds a political agenda and the formation of a specific kind of politics associated with secure communications; and a third interested in the generation of an economical value exchange system. Based on an analysis of the gears and technical functions of blockchain technology, I argue that the technical gears of the blockchain are strongly marked by its prehistory. Indeed, I suggest that Bitcoin is a technical embodiment of this (political) prehistory.

I then move to discuss literature surrounding the political weight of code and identify specific events where code and politics were strongly associated. Placing the prehistory of the blockchain within the context of this literature, allows me to argue that blockchains expand the performativity of code as a contender of state institutions, not only as a replacement for regulation and execution, but also as a producer and transmitter of economic value.

3.1 Bits and Pieces

Three trajectories are connected by two events: the first, a controversy surrounding the Pretty Good Privacy (PGP) protocol and software; the second, the rise and fall of Digicash, an early attempt to implement digital cash. The former is a moment where cryptography techniques came into conflict with government regulations, while the second is a practical attempt to create a state-independent form of money through cryptographic techniques.[29] These events should not be taken as indisputable seminal moments or “causes” that can be traced in a straight

29 Digicash was partly funded by the Dutch government, which sought a new payment technology for their transport system. The technology allowed to outsource the authorization of small cash-like payments from a fiat system to a cryptographic scheme, thus, susceptible for adoption by the Dutch government, but not independent of its institutional structures.

line of events up to the appearance of the blockchain. In fact, PGP is not part of the Bitcoin protocol (or any other blockchain to my knowledge), nor is any technical specification of Digicash. On the contrary, the failure of Digicash signals the discontinuity of this history. Instead of causal examples, these events should be read as representative moments where the main concern of a specific historical period is woven into the next one: in the first case the concern of cryptography with an anti-state political stance, and in the second, the synthesis of non-state cryptography with payment functionality. More examples that stress the continuity and discontinuity may be found in extended research of the prehistory.

The gears of Bitcoin thus are presented as a line of descent in the tradition of Foucault, Kittler and Media Archaeology. The material elements built in Bitcoin, e.g. the specific cryptographic technique used to hash information, are used to dig into a particular history of communications. Unlike Nietzsche's genealogies, which allegedly sought the origins of, for example, guilt, Foucault's take on genealogy aims to show how dissimilar practices and discourses are assembled to form, for example, the regime of incarceration (Lightbody 2010, 185). In the same way, my approach shows a particular thread of cryptographic, economic, and political elements that are materially knotted in Bitcoin. Friedrich Kittler takes up the genealogical and archaeological techniques of Foucault, but emphasizes the material weight of the medium. His seminal work on "discourse networks" (Kittler and Metteer 1992) considers the sociological conditions of literature as media, but stresses the role of media as provider of new forms of social relations, modes of memory, and the way devices offer new ways of perception. The term "discourse networks" designate not only the institutional arrangements but also the relevance of technological devices to allow society to select, store, and process information. For media archaeologist Jussi Parikka the two main contributions to media studies that Kittler brought were to observe 'old media' as media systems for institutionalizing information for on the one hand, and to decode the working of power in the current environment of technical media on the other.

I am not observing old media in the same exact sense as Kittler: the history of digital cryptography is relatively new, and my starting point is at the end of the nineteen seventies. Elongated lines of descent can be traced through the history of cryptography, e.g. Kittler locates the first uses of cryptographic methods to the Roman transition from Republic to Empire (Kittler 2008), and discusses the

importance of cryptography for the outcome of the Second World War (Kittler 1999). Unlike other archaeologies this line of descent looks at a brief period of time, compressed yet significant to explain the political positioning of the gears. But like Kittler I observe the pieces in relation to institutionalization of information. In the particular case of the "trajectory of manifestos", or the moment where tech-savvy communities antagonized state's control of cryptography, encryption as a medium was in a way re-institutionalized: the political struggle demanded the use of the techniques available for a broader public, and while the control was partially taken from state institutions, to say that it was de-institutionalized would be misleading. Instead, as I argued in the first chapter, notions of power performance, such as authority, are coded or re-institutionalized in software, protocols, and computational frameworks. In this line of thought my work also follows the Foucault/Kittler tradition that seeks to decode power dynamics within the digital media landscape. Finally, my research lingers in between the medium-specificity of Kittler and Hu's medium-agnosticism: I do not look at one technical object, but a series of 'trajectories' that include different technologies and diverse socio-political contexts; however, the Bitcoin blockchain, read as a specific material medium, acts as a reverse point of departure to trace this lineage.

This genealogy comprises the period from the early seventies to Bitcoin's white paper in 2008. The descent, as Parikka states, is not only historical but infrastructural: "Media archaeology goes back not only in time, but inside the machine" (Parikka 2012, 81). I will associate three different materialities embodied in the machine with each trajectory: technical gears, discourses, and projects. The technical gears listed in the trajectory of insecure communications are actual pieces or inherited versions of technology that take part in the code or protocol of Bitcoin. This machinery includes Merkle trees, Blind signatures, Elliptic Curve Digital Signature Algorithms (ECDSA), Reusable Proof of Works (RPoW), and the SHA-256 hashing algorithm. Then, the trajectory of manifestos considers some of the techno-political discourses that expressed the *utopian spirit* of the internet as a place unaffected by "real world" politics and, thus with the potential to create its own political frameworks. Three popular representative manifestos of the emerging cypherpunk culture are discussed: the Crypto Anarchist Manifesto, the Cyphernomicon, and the Declaration of the Independence of Cyberspace. Finally,

the trajectory of crypto-money gathers some of the partially successful attempts to create a digital version of cash or state- and industry-independent payment systems. Endeavours towards the creation of digital cash that culminate with Bitcoin include Digicash, Hashcash, B-money, and Bitgold. In some cases, Bitcoin inherited and applied specific techniques from these projects, others helped to set up the landscape where the idea of a distributed payment system was feasible. The threading of these trajectories sheds light on the assemblage of technical objects, concerns, and discourses, which became the condition of possibility for the appearance of digital objects like Bitcoin.

Secure Communications and the PGP Event

David Khan's (1996) seminal work on the history of cryptography, *Codebreakers*, identifies two core elements for cryptography that appeared in Egyptian civilization: a deliberate transformation of writing and the pursuit of secrecy. While he believes that its first uses of cryptographic techniques were aimed at increasing the mystery and magical elements surrounding religious places, such as tomb's epitaphs, a great part of the history of cryptography is embedded in the history of military communications. Despite its non-military uses, the interrupted evolution of secret communications that became the "deadly serious science of today" (Kahn 1996, 66) is constantly coded along military conflicts. This relation is not unexpected: military events benefit from a dedicated channel of communications for strategic purposes and are capable of gathering extraordinary amounts of resources to develop and expand secrecy techniques. The 20th century provided a fertile ground for the accelerated evolution and usage of cryptography by introducing mathematical formalizations into two of the biggest world-wide conflicts. Secure communications through cryptography was critical to the outcome of the Second World War, as exemplified by the successful decoding of German ENIGMA machines by Alan Turing's British counterpart, the COLOSSUS (Kittler 1999, 253), or the Japanese message disclosing the incoming bombing of Pearl Harbor that opens Khan's book narrative (Kahn 1996, 6). The use of cryptography for strategic and military communication continued through the cold war and into the present.

Bitcoin and all the subsequent blockchains are an expression of the cryptography that sprouted after being detached from its exclusive use in national security. They are also a modern solution for how to securely exchange information through cryptographic methods (the solution to the Byzantine Generals' problem mentioned in the first chapter of this work). The term "cryptocurrency" is the union of a unit capable of circulation, a currency, and the cryptographic techniques that allow for an untampered transmission. I will develop an account on how the connection between these two parts evolved. For the moment, I will briefly discuss how this exchange of messages works in Bitcoin.

Transactions within the Bitcoin protocol are the transference of coins —or any kind of token in other blockchains— from one owner to another. However, this should not be understood as an exact analogy to a payment made with non-digital money, or even with other digital payment systems. The tokens in Bitcoin are but a record of a transaction, information in a ledger. Arguably, this operates in the same way as the rest of non-physical money.[30] But the crypto-coin is made itself from information of current and previous transactions. It is not only an entry on a database, but an entry that signals a chain of events happening before it. These transactions are grouped into blocks, hence the popular "block-chain" label. The way in which a user can claim ownership of a coin, and thus having permissions to add new information to the registry in the form of new transactions, is through the use of digital signatures. The electronic coin is then defined as *a chain of digital signatures*. Signatures, like their ink-on-paper versions, serve to provide proof of the origin and integrity of a digital element, such as a business document. But the digital versions replace notarial power with mathematical proof, and are commonly used today, in particular since the emergence of asymmetric signatures.

Public-key, or Asymmetric, cryptography was implemented in 1976 by Diffie and Hellman (1976) as a solution for sharing a secret key without previous communications between the peers and even through an insecure channel or in a broad network. Their seminal paper acknowledges that the major problem in cryptography is privacy, thus their answer allowed making public one of the pair of

30 The amount of fiat money in the form of cash that circulates in the economy is 'insignificant' (Jessop 2015), compared to the credit in circulation: it is estimated that the former accounts less than 3 per cent of the economy, while the latter accounts for almost the remainder 97 per cent (Ryan-Collins, Greenham, and Werner 2014).

keys, while keeping the other private. Jean-Francois Blanchette (2012) discusses extensively the working and history of public-key signatures (without ignoring the history of its failures). He summarizes Whitfield and Diffie's brilliant but 'deceptively simple' system of key-pairs: "The trick lies in the mathematical relationship between the public and the private part of the key: although each key provides the inverse function of the other, even with significant computational resources it would require considerable amount of time to deduce the private from the public portion of the key" (Blanchette 2012, 43). The technique exploits one-way function problems: mathematical puzzles that are easy to prove for correctness but difficult to solve. Having both keys proves their unique relationship quickly, but having only one is extremely difficult to generate the other. This solution improved the effectiveness of cryptosystems by leaving behind the unreliable beliefs and heuristics and replacing them with algorithms and computational power, ultimately achieving 'provable security', a mathematically demonstrable type of guarantee (Blanchette 2012, 8). The technology allowed the exchange of securely encrypted messages between two parties using public available information (the public key), as long as a key pair remained private (the private key). In the Bitcoin system, the receiver of the coin generates a key pair, making half of it public. The other half is stored in an online or offline wallet. Whenever a person 'spends' a coin, they use their private key to sign a new one (and thus transfer the value). The digital signature of a payment resolves the part concerning the authenticity of the ownership and the authentication of the parties. From a technical point of view, what makes the action reliable is not the user choices or interaction as a person, but the coin as a chain of verified additions to the ledger.

Public-key cryptography exchange was later implemented in the RSA algorithm and broadly used for obtaining public keys and digital signatures (Rivest, Shamir, and Adleman 1978). Rivest, Shamir and Adleman are ahead of their time when they venture that their cryptographic method has 'obvious applications' for electronic funds transfer systems.[31] Bitcoin uses Elliptic Curve Digital Signatures Algorithm (ECDSA), a secure algorithm similar to the RSA but with a smaller

31 The RSA algorithm is another good example of the close relation between cryptography and the military. It was in fact independently discovered at the British Government Communications Headquarters (GCHQ) early in 1973 by Clifford Cocks, a mathematician working at the institution, but remained classified information until 1997.

footprint, which improves communication within its network. It uses a one-way function using big prime numbers, which means that it is relatively easy to read the coded message from one way and almost impossible on the other way around. It is based on DSA, a Federal Information Processing Standard (FIPS) proposed in 1991 by the National Institute of Standards and Technology (NIST), an agency of the United States' Department of Commerce (López and Dahab 2000). ECDSA is complemented by Merkle trees to generate new blocks on the chain with the minimal amount of information. Patented by Ralph Merkle in 1979 (Merkle 1980), Merkle trees are used in Bitcoin mainly as a technique to save space: transactions are hashed in a tree, and only the root (the addition of the branches' hashes) is included in the block resultant data (or 'header'). The use of Merkle trees is handy to authenticate a hash comprising a large set of data (Merkle 1980).

The *public* in public key is relevant beyond their technical affordances. It signals the dissemination of the cryptographic affairs to a broader audience, and the notion that good cryptographic techniques benefited from public scrutiny. For Blanchette, the cryptographic moment fuelled a debate (sometimes confrontational) over the control of this applied mathematical knowledge, which was previously solely under state control, and then reclaimed by the scientific community. What is more, Blanchette notes that the claim was grounded on a growing critique of a state's management capacity, and an incipient sentiment of moral responsibility on the tech-savvy community towards a fair use of crypto: "Cryptographic tools and knowledge would thus move from a dysfunctional institutionalist context dominated by the needs of states for self-protection, to one regulated by the scientific ethos of openness" (Blanchette 2012, 40).

The gradual separation of state and cryptographic techniques is clearly represented in the PGP event. Pretty Good Privacy (PGP) was a software created by Phil Zimmerman, a young cryptographer with the goal of creating a public software that allowed the practical use of public-keys. By 1991, Zimmerman was close to having a finished product. In the same year, a bill to strengthen antiterrorism measures was introduced to the US congress, it prohibited any kind of encryption inaccessible to federal government request. Zimmerman was pushed to publish and release his software through a young but blooming internet network. The dispute between the cryptographic community and the government is thoroughly narrated in Stephen Levi's (1996) work on the post-war history of

cryptography. The book's very title —"Crypto: how the code rebels beat the government, saving privacy in the digital age"— is evidence of the morally infused position of the cryptographic community towards the government. Zimmerman's has a significant place in the history of cryptography, not only because he managed to produce a working and efficient software for public secure communications, but also because of the symbolic role he played as a resistance towards the control of the state:

> Zimmermann's do-it-yourself effort to create a crypto program and distribute it to the people — an effort consciously undertaken to circumvent government control — marked a new dimension in the ongoing battle between the NSA and the cryptographers who worked outside its reach. The agency had once felt that its voluntary prepublication compromise with academics had mitigated much of the potential damage of that community's emergence (Levy 1996, 257).

In 1993 Phil Zimmerman was being accused of exporting 'munitions without a license' for having his PGP software distributed worldwide (Garside 2015). Strong cryptography —i.e. encodings that security agencies with substantial resources are unable, or struggle, to decode— was considered a weapon and thus not to be shared outside the country. However, the new materiality of software was different from that of a bullet: while the execution of the PGP program may be considered a weapon deployment by law, the diffusion of the source code was made possible through its slippery embodiment. Zimmerman exploited this and published the source for PGP in a book format, thus being able to export it. The code associated with cryptography challenged the government's role by exploiting its malleable materiality, and inaugurated a moment where this materiality was seen as a possibility for executing a different kind of politics. What followed was a period of manifestos claiming the blooming digital communications as a space independent of centralized politics.

Manifestos and the Digicash Event

The PGP event encouraged the political organization of the crypto-community to have regular meetings, mailing lists and the spreading of crypto

software (Barok 2011). The Electronic Frontier Foundation (EFF), an institutionalized association that sought to defend civil liberties in the upcoming digital age, was founded in 1990. The EFF is still active and describes its goals as: “EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development.” (‘About EFF’ 2007). It was founded by John Gilmore, Mitch Kapor and John Perry Barlow – hackers and technology enthusiasts with strong political positions. In the same line of thought, Timothy May (former physicist) and Eric Hughes (mathematician) devised the idea of a movement standing for a political libertarianism that enabled a technified society where anonymity was a crucial right. A meeting set to start such a group on September 19, 1992 (Levy 1996, 263) sprouted what was later known as “the cypherpunks”. May prepared a fifty-seven-page document for the gathering that would be known as the Crypto Anarchist Manifesto. The political tinge among the various early manifestations of Internet Governance was evident in the very format of the manifesto. The libertarian or sometimes so-called anarchist discourse standing for the development of techniques able to ensure the privacy and anonymity of the individual was set in a demanding and passionate form that emulated historical examples (such as that of Marx and Engels or the Futurists).

The Crypto Anarchist Manifesto’s (May 1996) first line is in fact a direct reference to the Communist Manifesto: “A specter is haunting the modern world, the specter of crypto anarchy”. Immediately after this rephrasing of Marx, it is stated that two persons should be able to exchange messages, make business and negotiate in complete anonymity, and that technology is on the edge of making it possible. In the same manner that, by creating the printing system in the middle ages, technology 'reduced the power of medieval guilds' and restructured social power, cryptography is bannered as the technology that will change the nature of corporations and get rid of government interference in our economic transactions. A year later, the Cypherpunk's Manifesto, proclaimed a similar set of beliefs focused on private interactions and encryption as the indication for the 'desire' for it. There is a straightforward position of distrust towards any institution that will offer privacy: “We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak” (Hughes

1993). The text ends by gesturing toward the possibility of a distributed system of governance, made possible by a dispersed system. A year afterwards, The Cyphernomicon, a second text by May was made public. This was an extended explanation for the cypherpunks group and mailing list. The section 3.4.1 (May 1994), concerning Beliefs, Goals and Agenda states:

- that the government should not be able to snoop into our affairs
- that protection of conversations and exchanges is a basic right
- that these rights may need to be secured through _technology_ rather than through law
- that the power of technology often creates new political realities (May 1994)

Even though not all members shared the occasionally extreme positions of the Cypherpunks mailing list's founders (May, Hughes, and Gilmore) most of them were drawn by the appeal of a right to secure communications. There are two implicit statements in the Manifestos: technology is more reliable than law, and holds the capacity to transform political reality. Code translates, among other things, directly as political praxis. In the words of May: “I don't see any chance that it will be done politically. But it will be done technologically” (Levy 1996, 200). This kind of proposition presumes the incapability of traditional enabled institutions to guarantee citizens' rights and challenges the (traditional) “code” on which they are structured; that is, it questions the law and the institutions that uphold and enforce it. At the same time, it is strongly confident about the capacity of the computational techniques to replace the old notarial code. According to Barok (2011), Gilmore expected a “guarantee – with physics and mathematics, not with laws – that we can give ourselves real privacy of personal communications”, while Hughes ultimate goal “was combining pure-market capitalism and freedom fighting. In his world view, governments were a constant threat to the well-being of citizens, and individual privacy was a citadel constantly under attack by the state” (Levy 1996, 259). But not everyone was subscribed to the ‘anarcho-capitalist libertarianism’: Phil Zimmerman, Hal Finney and Julian Assange, for example ‘were alien to it’ (Barok 2011, 5).[32]

32 The list subscribers included: “Adam Back, the author of Hashcash proof-of-work system; Julian Assange, the founder of WikiLeaks; Bram Cohen, the creator of BitTorrent; John Young of Cryptome.org and WikiLeaks ex-member; Hal Finney, the author of reusable proof-of-work system, and others who were directly involved in

The Cypherpunks mailing list was mostly active from 1992 to 2001, after which John Gilmore ceased to host it (Jeong 2013). The movement bloomed during the 1990s, an era of mass mediatization of the Internet. Its impetus resembles what i's identified by Wellman (2004) as the first stage of Internet Studies: an early period of utopian and dystopian visions. These visions are archetypically exemplified in Barlow's Declaration of the Independence of Cyberspace (Barlow 1996), which, resembling the tone of the previous crypto manifestos, stands against the intrusion of state governments and for the creation of an independent social contract and governance for the internet. This was the peak of the utopic moment for the newly opened "cyberspace". Code and transmission of information were the banners for a new, politics and enactment of rights, heavily infused by libertarian ideals. The cypherpunks mailing list mantra, "Cypherpunks write code", refers not only to the creation of technical tools through software development, but to the emancipatory power of technology and the potential to build a state-free society, or at least a landscape with less centralized control and fluid exchange of digital goods.

Kittler's notion of code stresses this dual meaning. On the one hand, he defines it as 'sequences of signals over time', based on a Wolfgang Coy definition ("from a mathematical perspective a mapping of a finite set of symbols of an alphabet onto a suitable signal sequence" [Kittler 2008, 5]), and as such, part of every communication technology and every transmission medium. On the other hand, it links code with its inherent historical function as a medium for the transmission of power. In fact, Kittler (2008) states that is in encryption were codes are materialized in the form of transmission of authority. He traces the origins of encryption to what was allegedly the first secret message system in the Roman Empire, in the letters of Julius Caesar and Augustus (according to Suetonius). Augustus is also credited for the creation of the first military mail system. Following an etymological pathway, he also notes that the Emperor's orders were called 'codicillia'. The term c*odex*, was used as "book". Thus, for Kittler: "the basis on which command, code, and communications technology coincided was the Empire" (Kittler 2008, 41). This meaning, according to Kittler, remained in the lineage of Empires until Napoleon, strongly associated with the

development of PGP, anonymous remailers, SSL, Linux kernel, or Tahoe-LAFS decentralised filesystem" (Barok, 4]. It must be noted that neither Chaum, Merkle, Diffie, Hellman, Rivest, Shamir or Adleman were, as far as I know, part of this particular mailing list.

book of law. Code was then the transmission of law, a circulating book of commands, rights and obligations. In this reading, code is a both a technique and a medium appended with command and law. According to Kittler, the use of the codex partly explains the success of Christianity which “took the historical chance, the technological leap” (Armitage 2006) to adopt this medium instead of the scrolled paper. In a similar fashion, the utopian manifestos claim the code as their own medium to design and transmit the laws of the upcoming cyberspace.

Lawrence Lessig links the fading of the post-communist euphoria of the mid-1990’s with the emergence of the digital utopias that promised a new exciting opportunity to develop new societies. The “cyberspace” expanded from universities to become a target for libertarian utopianism, where “freedom from the state would reign. If not in Moscow or Tblisi, then in cyberspace would we find the ideal libertarian society.” (Lessig 2006, 2). However, Lessig notes that the panorama that was being constructed ultimately become closer to an instauration of new kinds of control through code (like Galloways’ analysis explained in the first chapter of this thesis), than to an anarchic landscape. For Lessig, code acted as the new regulator, he famously paraphrased William Mitchell (1996) to encapsulate his view: code is cyberspace “law”. Lessing argues that code since the 90’s became the way a constitution is made, not as only as a book of rights and obligations, but also as architecture, that is, as the technical conditions of possibility for the development of actions and values: “What values should be protected there? What values should be built into the space to encourage what forms of life?” (Lessig 2006, 6). He ultimately asks that code raises the opportunity to ask which regulators we prefer. As I have argued in the first chapter, the current constitution of the Internet is largely centralized, the practical regulation on the web’s permitted uses and limits has and is being molded by a minority of actors, and the transition of control and authority to computational arrangements is not necessarily synonymous with an improved redistribution of power and authority, but merely a reconfiguration of it. But the landscape at the time was overwhelmingly positive, in particular for libertarian-related agendas.

The benefits of code for the construction of the political utopias were not only to act as a new command repository, but, as Wendy Chun (2013) argues, its inherent capacity to be put into practice. Like the orders coming from the Emperors, which were put into practice upon receiving the message, code has the

capacity to be its own trigger of power, it acts both as a passive recipient of information-law (such as PGP code source in its book/codex format), and as an active instantiation of command (such as the act of encrypting sensible information using the PGP software). Chun refers to research that theorizes code as performative element, such as Hayles' (2005) argument that code's performativity has a direct and causal change in the machine, unlike the human language, which relies on more mediated chains to have an effect (like the Roman messenger riding towards its goal with a piece of paper). This line of thought is also shared with works like Alexander Galloway's, as Chun identifies. For Galloway (2006), unlike natural languages, code is commands issued to a machine in a determined material substrate, and thus should be looked through an instrumental logic rather than a psychological one. Chun however, challenged Galloway's position by asking if code can be understood without being anthropomorphized at all: "How can code/language want—or most revealingly say — anything? How exactly does code "cause" changes in machine behavior? What mediations are necessary for this insightful yet limiting notion of code as inherently executable, as conflating meaning and action?" (Chun 2013, 23). Chun's reply to Galloway is that the mere use of high-level languages is already a way to anthropomorphize the machine by embedding them in "logic" and reduce actions to commands; for Chun, the fact that code is already enabling and disabling actions makes it a policing act. And it is this executability of code in the form of software that makes it really remarkable: "What is surprising is the fact that software is code; that code is—has been made to be—executable, and this executability makes code not law, but rather every lawyer's dream of what law should be: automatically enabling and disabling certain actions, functioning at the level of everyday practice" (Chun 2013, 27). What code embodies is an instance of performance of power that is traditionally assigned to bureaucratic law and other institutions of governments. For Chun, Lessig's famous adage "code is law" depicts the superposition of disciplinary and sovereign power, of control through a silent apparatus and through explicit submission of bodies. By following inherent hierarchies in the history of code and programming, like the work of female ENIAC programmers on one hand, and the resistance of "wizard" coders to a nascent automated programming on the other, Chun argues that code reworks power relations vertically: automation is populated both by narratives of liberation and empowerment.

This crypto ideologies of state emancipation eventually gravitated towards money. The second historical trajectory involves Digicash, the first implementation of an electronic cash system tuned to the cypherpunks concerns on freedom of information and the rights for privacy enabled through code. This event does not depict a direct causality towards Bitcoin, or an uninterrupted lineage from the cypherpunk movement. May's document for the first cypherpunk gathering already included discussions of "digital money in virtual realities", but in fact Digicash was already implemented in 1990, two years before the first cypherpunk meeting, and by 1999 —two years after Barlow's manifesto for the independence of the cyberspace, and almost ten before the creation of Bitcoin— the project had already declared bankruptcy.[33] The event, however, tied the techno-libertarian ideology with the intention to generate a stateless system for economic exchange. Its rise and failure inspired forthcoming attempts to achieve the very same goal, with Bitcoin as the most successful heir, itself stacked on previous efforts.

While the former cryptographic technology was concerned with general secure communications with possible deployments in, but not limited to, the financial field, David Chaum was the one who explicitly tied the two in a project to create digital cash. Despite being described as a silent figure who never attended a cypherpunk's meeting, posted to the mailing list, and even had a conflictive relationship with some of its members, Levi depicts Chaum as "the ultimate cypherpunk", "the privacy revolution's Don Quixote", and "the Houdini of Crypto" (Levy 1996, 267). Chaum's early paper "Numbers Can Be a Better Form of Cash Than Paper", opens with the following statement: "Soon, by accessing a computerized network from almost anywhere, you may be able to pay for a purchase, change your insurance coverage, or perhaps even send an electronic "letter" to a friend" (Chaum 1993, 174). The line already signals the hierarchical belief on the development of digital payments, which appear *even* more feasible than electronic letters. Chaum tied his thoughts on the technological with a recurrent political concern, for him cryptography was both an opportunity and a menace to privacy:[34] "Current developments in applying technology are rendering hollow both the remaining safeguards on privacy and the right to access and

33 For a close narrative of the rise and fall of Digicash, and an extended history of the development of non-distributed digital cash systems see (de jong, Tkacz, and Velasco González 2015).

34 Arguably, he even stated that 'the difference between a bad electronic cash system and well-developed digital cash will determine whether we will have a dictatorship or a real democracy' ('How DigiCash Blew Everything' 1999).

correct personal data. If these developments continue, their enormous surveillance potential will leave individual's lives vulnerable to an unprecedented concentration of scrutiny and authority.” (quoted in Levi 1996, 269). Thus, a great deal/amount of his efforts in the development of an electronic cash system were aimed at providing mathematical foundations for anonymity. Where others looked for a disconnection between authentication and secrecy, Chaum “sought to unlink authentication from identification and developed a series of cryptographic techniques whereby participants could perform information exchange protocols with surprising properties” (Blanchette 2012, 59). This led to the creation of “blind signatures”, a technique that enhanced privacy in public-key cryptography created by Chaum at the beginning of the 80s (Chaum 1983). Blind signatures enabled the production of verifiable signatures resistant to tracing by the original issuer, but keeping the transactional and proof verification characteristics. Chaum started Digicash in 1990, a company to develop his early ideas (going back to the beginning of the 80s (Greenberg 2012) on electronic money. The first implementation of his blind signature technology was ‘e-cash’, a smart card originally intended to provide easiness and security to the Dutch toll payment system. However, as a company, Digicash stalled. According to Eduard de Jong, security expert and cryptographer who worked with Chaum until 1992, the mathematical genius of Chaum did not match his marketing abilities and he failed to position the technology in the market (de Jong, Tkacz, and Velasco González 2015). Even though Digicash was a company providing a service and not an extreme anti-state bastion, and can be considered ultimately a failed project, it established for the first time a relationship between politics, cryptography, and money that would eventually make it possible for Bitcoin and other projects to come to life.

Crypto-Money

Digicash was perhaps the most relevant of the attempts to produce a cypherpunk-inspired electronic cash, but it was not the last. A year after Barlow’s declaration of independence appeared Hashcash, a proof-of-work algorithm designed by Adam Back initially as a mail anti-spam tool, but which will become

later an important part for the production of digital cash. Back's connection with the Cypherpunks ideals is not exactly surreptitious: his webpage, subtitled with the unequivocal motto “Cypherpunks distributed data haven” (Back n.d.), still has an archive of the Wikipedia entries on Satoshi Nakamoto, Bitcoin’s creator, and links to the cypherpunks mailing list and the personal webpages of Nick Szabo, Wei Dai and Hal Finney, all inventors of digital money systems. The role of Adam Back in the generation of Bitcoin is significant. The website *weusecoins.com* emphasizes Back’s figure on its ‘Who is who in Bitcoin’ section,[35] and Bitcoin's white paper (Nakamoto 2008b) recognized Hashcash as the basis for its proof-of-work to implement the decentralized timestamp peer-to-peer revision system. Back is in fact one of the few references used by Nakamoto. Although envisioned “as a mechanism to throttle systematic abuse of un-metered internet resources such as email, and anonymous remailers” (Back 2002), and not exactly as digital cash, hashcash marks the beginning of a short trajectory of crypto-money, the hotbed from which Bitcoin would eventually emerge. This trajectory is populated with successive attempts to create versions of digital cash systems: Adam Back’s *hashcash*, Wei Dai’s *b-money*, Nick Szabo’s *Bitgold*, Hal Finney’s *RPoW*, and finally Nakamoto’s *Bitcoin*.

Wei Dai is another of the scarce references in Nakamoto's original paper: he recognized b-money as a solution for the controlled decentralization of the transactions by publicly broadcasting them. Dai projected b-money in 1998, in the cypherpunks mailing list, as a currency system based on hashcash (DuPont n.d.). His system also generated coins by solving computational problems with the condition that these had neither practical nor intellectual particular value. The transfers functioned over a hypothetical 'untraceable network' where an anonymous user broadcasted a message declaring to give a certain amount of money to another. Then every node on the network updated its database by adding up and subtracting the quantity for each corresponding user (Dai 1998). In abstract, this functions as the actual Bitcoin network, since every node retains the whole blockchain and every transaction is publicly announced. Each node also sends the new block's hashes (with their transactions) list to its neighbours, and each node requests items they lack off from one another. Both systems also share the possibility for new users to use public information to synchronize with existing

35 He plays a significant role in the blockchain ecosystem up to this date, his role as co-founder of *Blockstream* is mentioned in Chapter Five.

nodes. But the b-money solution to deal with dishonest nodes was far from the technical elegance of the Bitcoin network. Dai proposed that each node should make a money deposit in a special account as a warrant in case of misconduct. This solution, compared with the automation that blockchains brought, was still too dependent on the centralization and human-management that the cypherpunk culture was trying to distance itself from.

Also in 1998 Nick Szabo proposed Bitgold. From that year to 2005 he developed his own decentralized currency, which was in many ways an important precursor for Bitcoin. It shared the idea of a chain and timestamped proofs of work, but instead of a one-way channel, it used benchmark functions: the resulting string of bits acted as a proof-of-work and was added to a public registry (Szabo 2005). This measure allowed some public control over the money generated, and therefore, the maintenance of its value. The reason for developing the system is then explained by Szabo's strong concern on the constant danger of inflation in fiat money economy systems (Szabo 2002). Szabo met Dai in a mailing list called libtech in 1998. According to Szabo the only people interested in these kinds of currencies, who overlapped 'cryptography experts and libertarians', were Dai, Finney, eventually Nakamoto, and himself (Szabo 2011). The year 1998 was the golden moment of the crypto-money trajectory (at least regarding the availability of proposals). Besides b-money and bitgold, in this year Hal Finney proposed the Reusable Proof of Work System (RPOW) with the goal of creating tokens of digital money, whose value was underpinned by computer resources. His RPOW system was designed to rapidly validate tokens that had taken long time to compute, with the addition of a sequential reuse (Finney n.d.). Finney worked previously with Phil Zimmerman in the first stages of PGP at the beginning of the 90's. In the same period, he met and kept up a correspondence both with Dai and Szabo (Finney 2013), both indirect co-designers of Bitcoin. He also received the first Bitcoin transaction, directly from Nakamoto, and mined block number 70 of the Blockchain. According to Szabo, at the earliest phases of Bitcoin, Finney was the only one 'motivated enough to actually implement such a scheme' (Szabo 2011).

It is crucial to acknowledge that many of the gears tools have been used, and still are, continually and for many ends. Some of them require the others -conceptually or in practice- to function, and are part of the daily invisible set of

tools that enable loading a secure webpage, signing into our Facebook accounts, or paying wirelessly with a debit card. None of these pieces is by itself quintessential for the particular function of Bitcoin. SHA-256[36], for example, is 'essential' to generate secure hashes, but not for making blockchain-enabled distributed token transactions, and in fact some altcoins replace it with alternative algorithms. There is, moreover, a chain of unsuccessful or experimental digital currencies (Mondex, Dancoin, Geldkarte, Chipknip, n-count, etc.) whose implementations date at least from 1992 to the present (de Jong 2014). The latter were more business oriented experiments than expressions of a political ideal, often developed with government aid and thus quite dissimilar to the cypherpunk inspired crypto-currencies.

The influence that each one of these systems early currency systems had on later ones varies, and so too does their adherence to the cypherpunk's political ideals (mentioned earlier). There are also a number of other trajectories and events that feed into the appearance of Bitcoin, like a growing interest in digital payment systems of all kinds; the global financialcrisis of 2008 and the bank bailouts that followed; a DIY culture that grew parallel with digital technologies; the availability and systematization of free/open/libre software and systems; and the decreasing costs of chips and other computational devices, just to name a few. What the former gears —RPoW, bitgold, PGP, etc— describe is not so much the instrumental conditions of possibility of Bitcoin, as the virtual environment —the techno-political assemblage— that settled to provide a proper setting for the emergence of the various blockchain manifestations. A secure communications trajectory, which provided affordable and relatively public cryptographic technology, followed by a manifesto's trajectory, which overlapped the previous trajectory to associate these tools with political directives, anticipated the moment where the former embodied the possibility of a politically charged digital money in the crypto-money trajectory. These lineages illuminate, by means of pre-historical research, the occurrence of Bitcoin as a cryptographically-enabled economic unit, not due to a causality of events directed to its creation, but due to the formation of fitting conditions. They help to establish what is 'expressible' —discursively and in practice— in written and code form.

36 SHA (Secure Hash Algorithm) family algorithms were suggested around the same time of the Cypherpunks Manifesto. But being standards designed by the NSA for secure communications, the technology did not participate much on the political disputes of the time. Bitcoin uses SHA-2, published in 2001.

After Bitgold, the crypto-money trajectory remained 'silent' for ten years. Parallel to the blooming of digital payment and digital cash systems, inaugurated by digicash and with its own history of successful integrations and failures, quiet discussions on how to deal with obstacles for a non-centralized crypto money scheme developed mainly in mailing lists. Improvements to Back, Dai and Szabo's systems were made one step at a time. It was not until 2008 that Satoshi Nakamoto, in the form of an academic paper, detailed the protocol for his system to avoid double-spending, as well as the first version of the code to implement such protocol. The political stance of Bitcoin as a device or of Nakamoto as its creator, was not explicit. While he acknowledges the importance of former attempts and the usage of previous cryptographic gears, the explicit espousal of a libertarian political position, for example, is not forthcoming in his white paper (Nakamoto 2008).

This is reflected in the early literature surrounding the new payment system. For Karlstrøm, Nakamoto echoed the sentiments of the libertarian community, but was never as explicit as other actors, like May: "Nakamoto has stated that 'It's very attractive to the libertarian viewpoint if we can explain it properly', and Wei Dai states it even more bluntly: 'I hope this is a step toward making crypto-anarchy a practical as well as theoretical possibility'" (Karlstrøm 2014, 7). While Bitcoin correlated with the cypherpunks ideals, Nakamoto never acknowledged this position. Barok suggests that the appeal for libertarians was thus more of a marketing manoeuvre:

> it can be considered a brainchild of cypherpunk core values: importance of anonymity, independence from the central authority, and freedom through free software. Yet it is unclear whether Nakamoto was on the Cypherpunks list or familiar with it. He did not adhere to the ideology of free market anarchist society in any of his messages posted between November 2008 and December 2010 (Barok 2011, 5–6).

More passionate, yet unfounded, opinions depict the ghostly figure of Nakamoto as a self-declared political banner in the fight against the state: “Satoshi emerges from the darkness of the digital underground to lead the masses in a brave new world against the banks, oligarchs and multinationals; all who benefit from our ignorance about the nature of money, our powerlessness over entrenched state monopolies and our obedience to the collusion of government and big-business.” (Boase 2013).

Bitcoin’s white paper, however, holds no explicit political stand or claim. It deals with a mere practical problem of double spend, unresolved by former electronic cash designs. The problem the Bitcoin paper specifically deals with is double spending, that is, the possibility for someone to use the same 'coin' to make two different payments (uniqueness, as copyright debates know, is a ‘troublesome’ notion in the world of digital production. It is explicitly addressed to the system of Internet commerce, which for most purposes functions well enough and, when dealing with transaction fees, its author explicitly acknowledges that the system is “based on open market competition”. But the real concern is one inherited from the long list of renegade cryptographers: “While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model” (Nakamoto 2008b, 1). Even if there is no political reasoning in the paper, there is an implicit critique of the centralized management of money by banks: “The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank” (Nakamoto 2008b, 2). The previous sentence expresses the distrust in banks (or companies) as centralized bottlenecks, that is, doubts are cast on the monopoly of transactions due the capacity of the institutions. This concern is shared with the cypherpunks, since both parts harshly question the capability and intentions of the institutions to operate the transactions.

Nakamoto solution against double spending was more elegant, from the point of view of code, than its crypto-money predecessors: its peer-to-peer network uses a unique proof-of-work chain to record and publicly broadcast all hashed transactions, which makes it computationally infeasible to act as a

“dishonest”[37] node. Even in the unlikely case that a 'bad guy' overpowered the network, such a person could only, by design, take back money he or she already spent. But then again, the design's rationale is not entirely technical and sometimes it resorts to a Kantian reasoning too: “with that kind of computing power, it is wiser to generate more bitcoins and irrational to scheme any other fraud or depreciate the network” (Nakamoto 2008a). There is an archetypically liberal reliance on the rationality of the subject and its freedom of action, even the problem of double spending is understood more as a practical issue than as a moral one. The transactions are either valid or invalid, and the pinpoint of a double spender does not have the intention of sounding “the alarm and catch the cheater. We merely adjudicate which one of the spends is valid (...) There is no reliance on identifying anyone (...) The credential that establishes someone as real is the ability to supply CPU power.” (Nakamoto 2008a). Subjectivity within the design of the cryptocurrency is inherently understood in the same terms of freedom of anonymity that its cypherpunks gears. Dai's text on b-money opens up expressing its 'fascination' with May's crypto anarchist ideas and he eloquently proceeds to say that within this particular cryptography realm “the government is not temporarily destroyed but permanently forbidden and permanently unnecessary (...) violence is impossible because its participants cannot be linked to their true names or physical locations” (Dai 1998).

Unlike extreme techno-solutionist positions, such as the idea that violence may be simply eradicated by introducing an anonymity variable within a network, Nakamoto maintains a more reserved position. When faced with the assertion that one cannot use cryptography to solve political problems he stoically answers: “Yes, but we can win a major battle in the arms race and gain a new territory of freedom for several years” (Nakamoto 2008a). Recent works such as David Golumbia’s *The Politics of Bitcoin* (2016) make a sound case for the influence of the libertarian ideology that surrounded Bitcoin’s design. But even if the political agenda of Nakamoto remains partially uncertain (as he left few traces, and remains unidentified as this text is being written), its government-emancipated mode of production and exchange nicely correlates with the market flexibility, code-enabled trust, privacy requirements, and state independence so highly valued by the cypherpunk and libertarian-alike community. And the affordance

37 Nakamoto expresses discontent with this term, probably because its strong moral semantics (Nakamoto 2008a).

brought by its design, i.e. the capacity to detach control of exchanges of circulation from the centralized figure of the state, resonated not only with the libertarian yearnings but also with any party interested in increasing fluidity in the market context. Karlstrøm states that Bitcoin is “at its core an attempt to expand the purview of markets through destabilizing universally adopted state monopolies on the production and verification of currency” (Karlstrøm 2014, 2).

For Sybille Krämer (2015) money plays the role of a state-controlled medium, and not only a symbol or embodiment of a social institution. For her, money acts as the abstraction of ownership that can be transmitted. Money is a medium between people, and does belong to a different category than other goods, as its value is detached from any materiality, it “embodies the disembodiment of value, it desubstantializes values. It is the objectification of an abstraction” (Krämer 2015, 113)). The idea of an objectified placeholder of value can be applied, following Krämer, to a symbolic value (e.g. the value of a commodity). However, the body that holds (by desubstantiation) the immaterial property must be nevertheless validated by a central entity. According to Krämer, the very fact that people are unable to produce or consume money without a central institution to validates its otherwise abstract value, shows the ‘otherness’ of money in relation to other goods. Bitcoin, as a currency-embodied blockchain phenomenon, allows the production of desubstanialized value without the figure of the state. According to Bjerg (2016), Bitcoin does not rely on the trust in the central authority of the state, because this kind of post-fiat money places its value in the trust of the community. On the contrary, I have argued in the first chapter of this research for the existence of a void of authority that is not filled by any particular set of players, and against the idea of the community as a main provider of value. Instead, the new capacity for distributed digital production, in the same sense as law and execution were previously developed, appends to the overwhelming domination of code, to “the conditions of possibility that software establishes” (Fuller 2008, 2).

The production process of blockchains is the essential novelty brought by these technological devices. Even if we ignore the element of an intentional confrontation with the figure of the state, embodied in central banks, the system of distribution through computation weakens previous authority structures of control. That is, the history and emergence of Bitcoin does put into play a coercive

relation with previous authority systems, regardless if that was its intention by design. What is at stake is a rearrangement of a power structure. Brett Scott has made a similar point when he suggests (Scott 2014) that in the current economy, banks are *merely* entities controlling the recordings of transaction data. Meaning that its privileged position in the current structure of power is linked to recording as a mean of control. Scott proposes to replace their databases and find a way for people to control them. For him the blockchain is already a solution for the first problem, but does not entail an answer for the second, as he emphasizes that digital-anonymous-decentralized-ledger systems are not by themselves a guarantee of good use or social growth.

Whether blockchain systems bring a democratization of control and production or merely relocate these elements towards a new minority of players is neither a settled issue nor an inquiry to be fully answered by the scope of this research. Instead, my argument in this chapter is that blockchain technology enhances the performativity of code for the replacement of previous socio-political institutional strongholds. Not only is it code as law, and command, i.e. as regulator and executioner, but also as producer and transmitter of economic value. The blockchain marks a transfer of authority from established institutions to code, and the authority expressed is built into the system itself, thus control and function overlap in the production of digital assets. The trajectories I followed departed from Bitcoin's technical blueprint to present a lineage that threads communications and political stances present in blockchains as current cultural phenomena. The "stuff of software" (Fuller 2008, 1), or Bitcoin's as an assemblage of techniques, is used as a springboard to tell the story of a genealogy that established the conditions of possibility for a state-independent exchange artefact. This research explains the emergence of a digital object (Bitcoin)[38] by dissecting its pieces and tracing their lineages, but it also expands into the further performativity of code that is expressed in other instantiations. Its prehistory is generative of a diversity of techno-political artefacts (e.g. *Ethereum* and newer blockchains) expressing the metaphor of *the blockchain*. This metaphor is fuelled by discernible historical claims —peer to peer circulation, distributed mathematical verification, and anonymous usage— that reconfigure code as law, command, execution, and production.

38 Bitcoin's evolution will be further discussed in Chapter Five, through observing its governance and design.

Chapter 4: The *Space* of the Bitcoin Network

This chapter explores the spatial and location characteristics of the Bitcoin blockchain. It inquires as to where the blockchain is *performed*, and provides an answer that draws upon the technical characteristics of the blockchain network. Through an exploration of the empirical operation of the network, I open up a broader discussion regarding the position of blockchains among new political geographies. I pay particular attention to the repositioning of the concept of territory, from a technology of sovereign power in the form of horizontal division of the space, to a technology of sovereign power in the form of flexible but controlled layers or stacks (Bratton 2016). The relation with the figures of state and with technology corporations, like in the former chapters, plays a significant role to understanding the specific performance of public blockchains, both as antagonists and allies.

The chapter opens with a brief overview of the internet infrastructure and its geographic issues. It is relevant to offer a brief context of the geopolitics of the internet, because a) blockchains are networks underpinned by the structure of the former, and b) they intend to mend privacy issues opened by the geolocalisation of this infrastructure. Then, a technical overview of the network distribution is offered: this consists in the use of technical tools to provide an overview of its nodes. This section shows the relevance of spatial analysis, as it shows how territorial constraints influence the production and transference of bitcoins, despite the attempts of the system towards full distribution. The analysis of the network shows that the network is decentralized but concentrated, and thus, materially locatable. This approach ultimately shows two different kind of “limits”: on the one hand, the network has its own concentrations and these concentrations are partially subjected to the traditional conceptions of territory and quit specific nations. On the other hand, the partial information that is possible to obtain through a territorial framework is limited, and thus, a different political geography is required to make sense of blockchains as a technological phenomenon.

Thus, I explore two approaches to think the relation of blockchain as a technical phenomenon with other territorial arrangements. I propose that blockchains diminish the relevance of earth topographies, but maintain a relation with geographically-demarcated states through standardisation processes, e.g. the formal agreement to use bitcoins to pay for services. I also note that another characteristic of blockchains are to expropriate the state functions of production and transmission of assets, thus partially competing with geographical states. These two relations stress the importance of a relation with state-nations, but also the non-essential role these play in blockchains development. I argue that in this technology, a claim for space, state competition, and the disappearance of the territory as a technology of power (Elden 2013) is embedded in the promise of frictionless circulation of assets. I end the chapter with the idea that the Stack (Bratton 2016) offers a better framework to think about the space generated and fulfilled with blockchains. The Stack is relevant as a geopolitical framework for the blockchain, as it allows the re-configuration of a post-territorial power structure, based on the internet as infrastructure, but that generates its own subjects and authority models. It interacts with the established state geographies and disciplinary models, but it is only partially subjected to it, and in doing so builds a distinct political geography with its own models (allegedly sovereign) of "computational" authority.

The overarching narrative of the utopia along this chapter exploits the most direct meaning of the word, based on its etymology: a no-place, or a place that is no-where. While the parts of the Blockchain (like the physical nodes that make up its network) can be located with some degree of specificity, a geographical or territorial approach does not properly describe the extension of the Blockchain. The object is itself paradoxical: it is neither universal nor immaterial, which means it can be located, but the way it performs its spatiality is no-where in particular. This utopic mode is more visible when contrasted with the territoriality performed by traditional political definitions of the state, and particularly relevant within the discussion of internet-enabled infrastructures fuelled by a rhetoric that imagines emancipation from territorially-based authorities.

4.1 Cyberspace and Territory as a Technology of Power

The notion of territory and political delimitations are strongly interwoven. Modern nations are limited by territorial borders and primarily identified as geographical units. Borders in the form of natural formations such as rivers or mountains, human-made constructions such as walls, and even invisible lines mark the formal limits of the *res extensa* of political clusters. Our current notion of territory is settled with modernity and the formation of the nation-state, however, geographical delimitations have a long history of ties with powerful political structures (Elden 2016). The early Roman Empire had less clear notions of a frontier, in part because it was thought as an ever-expanding imperial power without limit, (*imperium sine fine)*, growing throughout the whole world (*orbis terrarum*). Its "frontier consciousness" (Graham 2006) developed gradually and not only due to a topography-based military expansion. The perception of space was formed by a complex gathering of economy, strategy, defence and administration processes. The *limes*, or borders, were seen as administrative jurisdictions in the fourth century (Isaac 1988) than as a hard limit of the boundaries of empire (imperii fines). According to Graham (2006), what was earlier thought as a division of regions and people, evolved from the third to the fifth century to an idea of a territorial frontier.

The separation of the earth, following these readings, was tied more to a notion of authority related to the control of goods and people, than a sovereign demand upon land. Stuart Elden argues that the notion of territory as a sovereignty technology was fundamentally developed by late Western politics (Elden 2013). Elden focuses on historical political writings regarding law, land, and empire to show that authoritarian and sovereign claims were made upon land and people but not on the full modern notion of territory as the legal control of a delimited space. It is not until Leibniz's definition of the sovereign as he who is 'master of his territory' (Elden 2013, 320–21) that the territorial notion of the control of space is produced. Elden's interpretation adds a genealogical approach to previous seminal works that understand territory as a social construct aiming to influence people, relationships or other phenomena via the control of space (Sack 1986). Benjamin Bratton (2016) pinpoints the modern design of territorial nation-state in relation of jurisdiction at the 1648 Peace Treaty of Westphalia, which

ended the Thirty Years War. The Peace of Westphalia was based on an agreement of co-existing legality in between states, a shared European political order based on territorial sovereignty. For Bratton, this agreement inaugurates a global design of geopolitics based on planar geography, the result of a process of "separating and containing sovereign domains as discrete adjacent units among a line and horizontal surface" (Bratton 2016, 5). Following this line of thought, I will understand territory primarily as a technology of power. This may be related to a modern notion of sovereignty through control of land, but also to older understandings of administration and control of topographical spaces.

Understanding territory as a technology of power opens interesting questions on the territorial characteristics of technologies arguably, apparently with a good degree of success, are defiant of territorial constriction. The bitcoin network is a contemporary example of this, but it is certainly not the first. Internet, the network on which Bitcoin relies, has a complicated history with space or, better said, with the idea of a lack of it. I'll offer a brief commentary on how the idea of the internet as a no-place, or as a space unreachable, got entrenched with traditional state geographies. This internet commentary is relevant because of two reasons: first, the bitcoin network, like many other protocols and platforms, is built on the basic infrastructure of the internet. It works over it, and thus is affected by both its affordances and shortcomings. Second, as much as it is based on the internet, it is also an attempt to go beyond it. Not only because it offers the novelty of private digital assets on distributed networks, as I have argued in the first chapter, but also because blockchains can be read as a reaction to the control the internet yielded to traditional regulation. As I argued in the previous chapter, Bitcoin is the partial manifestation of an ideology that sought independence from centralised state controls. And while the internet infrastructure was always developed and controlled by national authorities (the US in particular), the autarchic ideals that it sprouted during its early mediatisation, resurged in the goals of distributed ledgers. To different extents in each embodiment, decentralisation, privacy, anonymity, and frictionless exchange were kept as main goals in most blockchain phenomena. From a territorial point of view, as the internet increasingly resembled an outline of a Mercator political geography, blockchains tried to reclaim this alternative, *internet-derived* idea of space (Toor 2013).

Cyberbalkanization

The notion of 'cyberspace' as a non-defined or borderless region outside traditional ideas of land, state and regulatory institutions was a primordial characteristic of the Internet of the 90s, both for their savvy insurrectionists (Barlow 1996) and for the 'extramedial' (Chun 2008) representation of the then confused newcomers. The “virtual nonplace”, defined by Wendy Chun as “a place in which things happened, in which users’ actions separated from their bodies, and in which local standards became impossible to determine. It thus freed users from their bodies and their locations” (Chun 2008, 37–38). If understood as infrastructure (hardware and protocols), Chun considers it unmappable. However, if understood as high-level script languages, it is understood as *spaceless*, since these languages (e.g. HTML) aggregate objects without a continuity in space (see Manovich 2001). To better understand (and further complicate) the notion of cyberspace, Chun contrasts “place” and “space”. While the former designates a finite location, the latter is more of an interval. Based on their etymologies (Place, *platea*: broad way; Space, *spatium*: period), Chun argues that *place* is more related to notions of civilization —of territory, as discussed before—, and *space* to freedom or unconquered possibilities. She strengthens these conceptions with the aid of Michel de Certeau’s, who thought of *place* as a stable relation, and of *space* as those relations in action. The latter is an experienced map, a route. Cyberspace, Chun argues, loses both notions: place loses its stability, websites move and disappear, or are modified depending on the visitor. Cyberspace is also not routable in the same way that space is: we never really navigate the internet, but an interface that crosses through it. However, even if we do not navigate packets of information in the way routers do, we do reformulate our relation with space within cyberspace: “By moving from URL to URL, we cut the scenery or space between fixed locations, while at the same time experiencing this ‘gap’ as an often unbearable space of time, in which we decipher the page that emerges bit by bit on the screen” (Chun 2008, 47–48).

There is an obvious reformulation of space after the internet. But the popular notions of what was enabled by it were commonly less sophisticated than

Chun's interpretation. As mentioned in Chapter One, the utopian tinge of cyberspace may be seen as a preservation of the sentiments of political utopias left by communist ideals (Lessig 2006), even though these are steered towards quite different economic models. Likewise, the utopian element of cyberspace as a no-place that was popularized through the 90s and early 2000s resembled more the "freedom" discourses of the internet manifestos. Not so much as a cognitive or ontological restructuring process of our notions of space, but a claim for unconquered territories, and thus as new frontiers carrying the promise of a different political and regulatory sphere, untouched by previous regimes' materiality and law. And while today most of our everyday interaction with the digital is highly centralised and locatable by default (e.g. Amazon data centres, and geolocation as a predominant characteristic of most internet services) a rhetoric associated with the digital as immaterial no-place remains, even if somewhat diminished. Extramedially, the 'virtual' and the 'cyber' as terms synonymous with the no-space debris endure, as one can confirm with the occasional newscaster or many informal talks. However, the 'end of the virtual' (Rogers 2009) has been sang from several fronts within the academia. Different methodologies have been developed to map a notion of space within the Internet, intelligible to social sciences point of view. And it has been partly because of these mappings that some of the immateriality and spacelessness has been debunked, or rather, reformulated.

Rogers (2012) identifies three stages of the Internet with their own political mapping: the early non-localised hyperspace, the spheres, and the networks. Hyperspace is hardly concerned with the territory but with navigation (in the early stage of virtual versus real opposition there is 'no place' for a territorial notion typically associated with land). Notions of space in the hyperlink era are made via possibilities of movement. The user clicking a link was as concerned of the in-between area of his point of departure and arrival as Han Solo pressing the hyperspace button on the Millennium Falcon (Lucas 1978). Methods for identifying the politics of the web followed the links too: these were understood as acts of association, as Rogers argues. Organisation started tracing the idea of secular spaces on a former endless cyberspace. Politics of inclusion and exclusion were identified with the first attempts of hierarchy classification made by search engines and directories, like Yahoo and Altavista, to mark sites authority

and reputation. Interesting cracks on the web's splintered surface were generated as a response to engines and directories in the form of blogs. By the decade of 2000 the Internet is understood extramedially and in non-empirical studies as a space of debates with a 'deliberate democratic spirit', and an acknowledged separation of interests and conversations: the blogosphere, the web sphere, and the news sphere. However, this separation was much more marked by a lack of debate (Dean 2002) and the creation of unrelated regions of opinion by the users' tendency to visit and encourage blogs, chats and forums with their own ideologies. This has been called *cyberbalkanization* (Sunstein 2009) and, perhaps more accurately *political homophily* (Ackland and Shorish 2014) since I am reluctant to identify it as a "natively digital" phenomenon.[39] This endures in one way or another, augmented today by what is popularly known as 'filter bubbles' (Pariser 2011), less related to human political contingencies and more to algorithmic-enabled user behaviour control aimed for web markets (Gerlitz and Helmond 2013).

Parallel to Internet's regionalisation of ideologies, a more traditional territorialisation enabled by technical means and standards was also developed: users and contents were separated by country codes. Communication between source and destination, client and server, is now played by regionalised rules: a French user may be unable to stream a song of a Russian region in the same way that a Chinese user may not be enabled to read news from other countries. This second kind of balkanization, also called *cybersegmentation* (Sassen 2002), developed in the last decade mainly due to two reasons: language and business (Goldsmith and Wu 2008). Being a global phenomenon, the Internet is populated by a significant proportion of non-English speaking users (2/3 in 2005). Thus, websites intent to address local needs, including the language, in order to offer a product, i.e., 'Youtube Philippines' has a slightly different offering than 'Youtube Canada', and its advertisement and popular videos are focused locally. The same applies to search engines and social networks. A mix between legal considerations per country, language zones and business as usual has shaped a quite territorialized contemporary Internet. Recently, a third reason forced once again a visible collision of the Internet and the nation. In 2013, Dilma Rousseff, president

39 Subsequent studies consider it a natural effect of one or another popular ideology leveraging on the network (Ackland and Shorish, 2009). For a compendium of studies of political homophiliy on the Internet see (Maeyer, 2013).

of Brazil, ordered to strengthen her country's online independence as a response to leaks proving that the National Security Agency (NSA) had intercepted her personal communications, the state-owned Petrobras oil company's network and Brazilians users of Google, Facebook and other U.S. companies (Brooks and Bajak 2013). President Rousseff proposal does not ban users willing to reach content outside of the country (as the case of China's firewall), but to store locally its data and to construct a direct underwater optic cable to Europe in order to avoid traffic necessarily going through U.S. servers. Territorialization due to surveillance has not alerted just Brazil; Germany is also trying to keep its citizens Internet and e-mail transmission constrained within its own landlines (Birnbaum 2013). Balkanization of the Internet works on different levels and for different reasons, but in a lot of cases responds to the nation-state's concerns on the “ideological control over the circulation of both its citizens and their capital in diaspora” (Barry 2001). President Jiang Zemin justification for the harshly criticised Chinese censorship grounds explicitly on the protection of their citizens: “From beginning to end, we must be vigilant against infiltration, subversive activities, and separatist activities of international and domestic hostile forces” (*BBC* 1998). This discourse is not limited to typically firewalled countries, as Cameron discourse to justify the £800 million investment on intelligence and surveillance to avoid cyber-attacks, among other 'challenges of today', reveals: “The enemy may be seen or unseen. So, as the Strategic Defence and Security Review in 2010 made clear, it is not massed tanks on the European mainland we need, but the latest in cyber warfare, unmanned aircraft technology and Special Forces capability (...) the plain fact is that in the 21st century, you cannot defend the realm from the white cliffs of Dover” (Cameron 2014). There is clearly a huge difference between the UK and China policies on censoring networks. The latter has outspokenly enabled severe state controls for some decades, to the point that it is reasonable to consider China's digital space not so much a 'censored' Internet, but only a different and partly separate network altogether (Goldsmith and Wu 2008, chap. 6). An Internet on its own kind, with a parallel development and its own particular kind of spheres. But even considering this divergence, it is important to stress the globally spread similarities on the defensive discourse that justifies increasing degrees of digital control.

Chun identifies the most idyllic moment of the Internet before its privatisation, when it was mostly in control of the US government —not without irony, considering the historical antagonism towards state shown in the manifestos — a period when "commerce was forbidden and TCP/IP developed with little regard for 'security,' since the 'community' of users was small and select (...) The disappearance of publicly owned, publicly accessible spaces (where publicly owned means state owned) and the concurrent emergence of publicly accessible, privately owned spaces has driven the transformation of public/private to open/closed" (Chun 2008, 38). The emergence and rapid growth of digitally native corporations (e.g. Google, Apple, Amazon, Facebook) changed the landscape of the internet ecosystem, making most of our spatial interaction in it crossed by private platforms. Not only the circulation of information is dependent on private telecommunication players (such as Network and Internet Service Providers, like Virgin or Verizon), but the interfaces for this infrastructure are exponentially centralised by private corporations. As an example, three of the five the most downloaded apps of the Apple store during 2016 (Eadicicco n.d.) are owned by the same company: Messenger, Instagram, and Facebook (being Snapchat and Pokemon Go the other two). If one considers that Facebook also owns Whatsapp, the most popular messaging service outside China with 900 million users(Sun 2017), and the fact that its main platform reportedly gathers over 2 billion users (Welch 2017), this corporation alone centralises a great part of the day to day internet traffic.

Geolocalisation plays a significant role for the enhancement of its services and the accumulation of data. Not only for social media giants, practically all new internet services exploit the localization of the users. Not only as a necessary strategy for the basic function of the services (e.g. Tinder or Uber as location-based apps), but as exploitable data for analysis or profitable asset (e.g. Snapchat does not require geolocalization to operate, but its disclosure is a condition to use the face filters, one of the characteristics that made the service so popular). In this reading, language, ideology, market, and international security all play their part in the fragmentation of the web.[40] Some of these elements, like security and free markets, resonate with many of the discourses on Bitcoin's emergence discussed in the first chapter. The actions and reactions of cyberbalkanization of the

40 Unlike Wu and Goldsmith, I do not consider language as an account for regionalisation since it is, at least in these examples, underpinned to marketing ends.

cyberspace are a continuum of the struggles depicted in the last chapter, and show the evolution of internal contradictions of the libertarian ideals in action. The new world utopia, the vision of an Internet unreachable and unchartable for more than its self-declared regulations (see Chapter Three), generated its own forms of regionalisation for the sake of business and market fluidity: the Initial Public Offerings (IPO) of Facebook, Google and Snap Inc. generated a lot of anticipation by merging the platform business model based on exploitation of data with more classical Wall Street-style public investments. The contradiction is that the business model of the modern internet is based on surveillance. Perhaps unforeseen by the internet manifestos sentiment, their claim for anti-surveillance clashed with the profitability of platform markets.

It is in this state of affairs that the Bitcoin network appears, carrying the proposition of a decentralised and frictionless digital exchange, yet also reviving the anonymity and non-spatial ambitions of the utopian internet moment. Proposed as a state-independent open protocol, the networks enabled by public blockchains have the capacity to theoretically operate outside of any territorial jurisdiction, and as a community-driven project, thus also independently of corporation-alike institutions. Furthermore, besides their non-territorial capabilities, the blockchains revitalised the promise of exchange communications working in parallel to complete or partial user privacy. However, as I will show in the following sections, the Bitcoin network replicates and renews internet geographical issues, but at the same time participates in novel understandings of the digital space.

4.2 The Bitcoin Network

While internet standardisations eventually signalled territorial-state marks (e.g. the .mx DNS code for websites related to the Mexican territory), or effectively produced an ecosystem tied to territorial borders, the Bitcoin network successfully maintains a less clear geolocalisation. However, it remains a phenomenon that can be localised, that is subject to indirect territorial regulations, and that develops strategical relations with nation-states. I will first show how the network can be geographically thought, by building a map of its technical workings, and sort the

relationships it inevitable generates, both organic and antagonistically, with territorial states. This section attempts to show, through technical means, that the network is decentralised but concentrated, and thus, materially locatable. However, in the last section I will also argue that the kind of network that blockchains enable are part of a new stage in the history of digital networks and notions of space. And that while the Bitcoin blockchain generates symbiotic relations with territorially-defined states, they ultimately adhere to a different political geography.

Coinjar, one of the multiple Bitcoin start-ups, moved its headquarters about 17,000 km, from Melbourne to the London docklands on December 2014. Although the main reason for the move, according to its CEO, was the 'progressive' ambience for cryptocurrencies in the London scene and the company's intention to become global, it was acknowledged that UK's more permissive regulation was also a sounding motive (Spencer 2015). Indeed, four months before, the Australian Taxation Office (ATO) published a guide for digital currencies, in which Bitcoin was considered a barter for users transacting less than $10,000 Australian dollars, but a commodity for businesses or quantities above, and therefore subject to a 10% Goods and Services tax when selling or buying it. The metamorphism of this curious digital object is by itself interesting, since between the new tax and Coinjar British headquarters a welfare application for the Australian government included a clause to declare 'cyber currency' assets. The financial categorisation in which these assets are located resembles a known Borges chimera, for it included time shares, race horses, taxi plates, greyhounds, traveler's cheques and collectables (stamps, art, wine and fishing licenses). For Jason Williams, head of Australian chapter of the Bitcoin Foundation (Bitcoin Association of Australia) this outcome was positive because not only the cryptocurrencies are recognised by the government, but also acknowledged as a form of wealth (Southurst 2014). Leaving aside, for the moment, the peculiarities of emerging cryptocurrencies' definition and regional regulation, what I find remarkable here is the *transoceanic relocation* of a finance company dedicated to transactions of a decentralised money 'that breaks down barriers'[41]. On its most basic description, "Bitcoin has no central servers for transaction processing or storage of funds (...) Bitcoin uses a distributed public universal database spread through a decentralised peer-to-peer

41 According to a Pete Williams (Deloitte Centre for the Edge) quote that figures in Coinjar's website https://www.coinjar.com/.

network" ('Bitcoin Wiki' 2015). But exactly in what sense is Bitcoin universal? For even if its universality claims are a mere exacerbation of its potential, and cryptocurrencies are not universal in a strong sense but distributed, how exactly are they distributed? Where do they stack and why? Why do companies invested in the promise of ubiquity perceive benefits in moving from one territory to another? Where are its *unbroken* or unbreakable barriers? And what kind of agencies mutually interact to define a frontier? For example, how does the lack of regulation or, on the contrary, the acknowledgment by a government diffuses or marks down cryptocurrencies' own space?

These questions rapidly highlight three things I will address: materiality, space, and limits. Like many digital devices, a sharp image of the object is unattainable; but like few of them, it presents itself as a user interactive device (i.e. a currency), although there is no fixed interface for it, there is no website containing the object, the only token is a string of numbers. It is possible to manage Bitcoin transactions via an ATM, a website, or a terminal emulator, in any case, there is no standard physical instance of it. This section clarifies the material notion of cryptocurrencies by providing a selected overview of the infrastructure of the Bitcoin network. Towards it, a map of the network, and its surrounding material actors will be charted. This leads me to my second highlight: the necessity to draft a space enabled by the device (or where the device comes to being). The prism for this approach is then first located in the order of the geographical; more specifically, the physical territory that the bitcoin network encompasses.

Nodes and Layers: A Map of the Bitcoin Network

Part of what comprises Bitcoin is a 'dedicated network' where every transaction gets processed, validated and stored, and it is the (technical) condition of possibility for cryptocurrencies prevalence and success. As a part of a broader attempt to build a Bitcoin space, an approach to the technical network will show how the network distributes in the world during a selected period. Addressing the bitcoin network can show the materiality (the hardware) of its nodes and edges. Since the network underpins the whole functionality of the device (in any of its embodiments: currency, storage, etc.), to emphasise this importance of this

material substrate is also to debunk any representations of Bitcoin as immaterial. I will also directly question the discourse of universality by showing the geographical specificity of the network's machines. The bitcoin network has previously been analysed through its transaction dynamics (Kondor et al. 2014; Baumann and Lischke 2014) and its anonymisation limits (Biryukov, Khovratovich, and Pustogarov 2014), but there is no geographically-driven study of which I am aware. A geographical point of view, will allow me to show where the network is shaped through technical mean since its function relies on the multiplicity of its nodes. That is, at the level of the network itself. This will clarify where exactly Bitcoin has an extended support. I will argue the Bitcoin space, via its physical network, has clear geo-located limits and death zones, but not necessarily tied to geopolitical stances. That is, the network has a material geopolitics, but this does not align straightforwardly with the territorial forms of governance particular to nation states. Departing from the idea that a decentralised network has no unique centre or at least no starting point, I will start tracing this network from a machine (or node in the network) where the software —which contains the information protocols to establish a communication with other nodes— is freshly installed.

When the software (Bitcoin Core) runs, it looks for peers in order to ask for a database of the rest of the nodes. The Bitcoin Core comes with a list of 'seed nodes' to query this database. In October 2014, the software code (v. 0.9.0rc1) had seven seed nodes which now will be discussed[42]. For a brief procedural moment, the new node sees a decentralised but not distributed map of the network.[43] Querying exclusively the seed nodes happens only once, afterwards, queries are made to all the nodes of the latest retrieved database. Since all the nodes are processing this operation constantly, once some nodes start communicating between each other, the seeds may be ignored and their importance flattens. The system then becomes a distributed network in relation to queries: all nodes can communicate with each other and share the same information. Despite its ephemeral status, it is interesting to note the geography of the proto-logical map of the seeds: three nodes are in the west, central and east side of the US (San Francisco, and the outskirts of Denver and Atlanta); one in

42 One seed node location is missing, the rest were obtained using GeoLite data by MaxMind. Which claims a reliability of 81% of correctly resolved IP's geolocation within 100 km (https://www.maxmind.com/en/geoip2-city-accuracy).

43 On the distinction between distributed and centralised, see Galloway (2004); Baran (1964, chap. 1).

Canada (London, Ontario); one in the UK (Ince-in-Makerfield, right between Liverpool and Manchester); and one in China (Hong Kong). This geography replicates to a certain point in the health status of the distributed rest of the network.

Part of the promises of cryptocurrencies is to be globally available to everyone, the code is open and different clients can run in almost any contemporary computer. The bitcoin network is, from an instrumental point of view, essentially formed by its nodes, thus the mapping of these entities can provide a good image of its geography. However, not every machine strictly qualifies as a node. These are any type of machine capable of running a piece of open source software (i.e. 'Bitcoin Core'), which allows them to receive, send and storage information of all the transactions. This network of machines is what makes possible the efficient running for Bitcoin transaction of information.

Nodes can be broadly categorised as 'full nodes' and 'lightweight nodes'. The latter are just clients that send and receive payments without storing the full blockchain and therefore, participate on the transactions but not on the maintenance of the infrastructure. A lightweight participant is the equivalence of a credit card user making a payment: his resources' information travel on a surface of which he is not responsible. The credit card has no value on it, if it disappears, nothing but a piece of plastic is lost. The card's sole function is to be a secure authorisation key to make changes to a ledger. The latter is the money. When the ledger subtracts an amount from one place and adds it to another, money is lost or gained. But beyond giving its approval, payer and payee take no part in what is completely a third party standardised administrative action (de Jong, Tkacz, and Velasco 2015). Both the ledger and the tracks where this information transit belong to different agencies (banks, governments, finance institutions of all kinds), but not to the card user. In this sense, Bitcoin works a lot like old and ordinary finance systems: a Bitcoin user may lose his or her phone or laptop, but the resources are still in the ledger, and as long as he or she keeps a copy of the secret keys, which are a cryptographically developed form of identification, the satoshis[44] can be reclaimed. The lightweight node approves transactions to be made to the ledger, but neither makes the changes nor helps in distributing the transmission of transactions. A full node on the other hand is responsible for the relay and

44 The smallest possible unit of a bitcoin.

validation of blocks of transactions, and its resources provide storage and bandwidth for the network's upkeep ('FAQ - Bitcoin' 2015). Unlike traditional registry administration, here the ledger is legion. Every full node contains a 'copy' of it (with no original) and validate its transactions. They are the structural skeleton of the network and the condition of possibility for users and transactions, therefore playing a crucial role in the endurance of the digital phenomenon of distributed cryptocurrencies. Interestingly, nodes don't need to be users of cryptocurrencies, they can help the network without ever receiving or sending bitcoins (unlike the miners, nodes receive no economic stimulus for a severe machine-demanding job)[45]. Miners are a kind of node specialised in collecting new transactions into blocks and require specific hardware and working conditions to do it; given its particular role in the bitcoin ecosystem, I differentiate them from regular nodes. The distinctions I am making can be summarised as follows: (1) A node[46] is not necessarily a user of the bitcoin currency, (2) a user (or lightweight node) of the bitcoin currency is not necessarily a node, (3) a node is not necessarily a miner, but (4) every miner is a node.

It is possible to set up a bitcoin server to act as a listener of other broadcasting nodes. Bitnodes website, supported by the Bitcoin Foundation, provides an API for one of these kind of servers[47], which makes possible to retrieve a limited amount of information about the network at any moment. With the intention to achieve an overall observation of the network behaviour, I set up a machine that continually collects and stores this information from it. In order to keep the data as complete as possible, the scripts run in a low-cost, dedicated 'raspberry pi'[48] machine, that is permanently connected to the Internet. The retrieval of information is made by a simple script that makes a request of the hostname of the server, country code, city, latitude, longitude, time zone, ISP, user agent, height, last connections, and the protocol version, for every node connected to the network. This simple python script retrieves new 'snapshots' of the whole network every 5 minutes. New 'snapshot' data is timestamped and

45 The Blockchain weights over 30 Gigabytes at this point, synchronisation requires significant bandwidth and energy, considering that it has an effect on the network only when it is connected.

46 Henceforth, by nodes I will refer to full nodes unless otherwise stated.

47 The code and instructions to set up a forked server is available at https://github.com/ayeowch/bitnodes. The information gathered by the API is, however, the same as the one gathered by setting up a personalised version of the server.

48 raspberrypi.org.

stored in a separated json formatted file, for later retrieval. Every snapshot can be read as a static moment of an ever-changing map of the physical network, containing all the nodes locations conforming the network at that moment. Gathering around 160-190 snapshots per day allows me to zoom in on how the network changes on a daily basis and over longer durations. Through more python scripts I generated sets from this data that were not evident or immediately retrievable through the Bitnodes API.

Using a second python script, for example, I queried and produced sets of 'strong', 'weak' and 'ghost' nodes, being respectively the machines that have been part of the bitcoin network uninterruptedly, interruptedly, and less than one day, respectively, during a certain time span. This allows me to propose categories of commitment or interest directly related to geographical zones. Full nodes for keeping the network healthy are becoming more and more scarce, support for the network has decayed since its highpoint at the end of 2013. There is even an incentive program[49] that provides a monthly amount of money to nodes that accomplish certain criteria to be considered highly healthy peers. Following this thread, I observe and classify different degrees of *commitment*, as an indicator based on continuity: I consider *strong* nodes those who are connected at every moment of the sample (in red, on the following figures), *ghosts* nodes those who are connected in less than 10% of the moments in the sample, and 9 levels of *weak* nodes, being 'weak9' the nodes present in 90%-99% of the sample, 'weak8' those present in 80%-89% and so on. Strong and weak nodes are a minority in the sample network, which is mostly composed by ghosts (fig. 1). The broader the sample, the more predominant become the ghosts. As fig. 2 shows, an extended sample considers 1317 continuous snapshots (around a week of data) from which a mere 4.3% nodes are strong, a small sum compared to 69.4% of ghosts nodes.

49 Interestingly, although this incentive is received in bitcoins, therefore using the network, the amount is not: it is a fixed sum of legal tender. More information at: https://getaddr.bitnodes.io/nodes/incentive/.

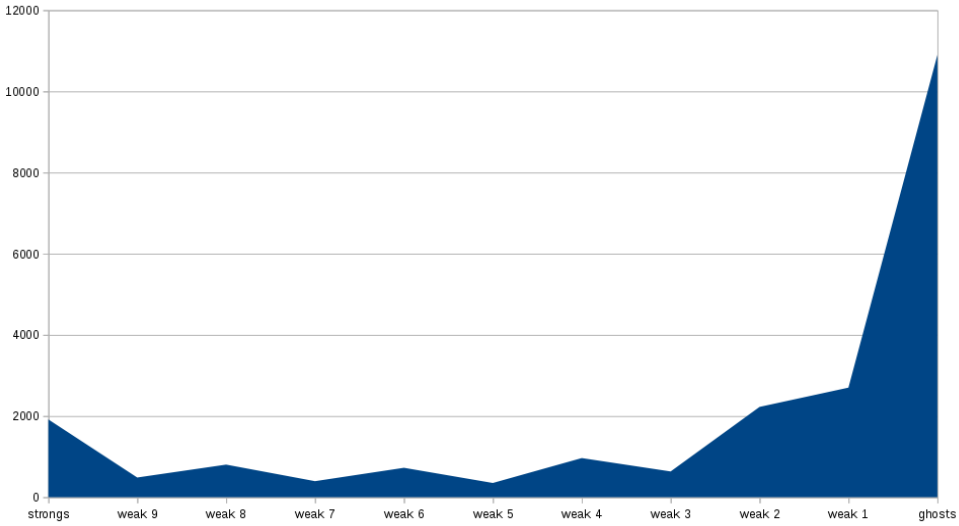

Fig. 1: Distribution of strong, weak and ghost nodes from a random sample of 15 'snapshots' of the network between March and May 2015

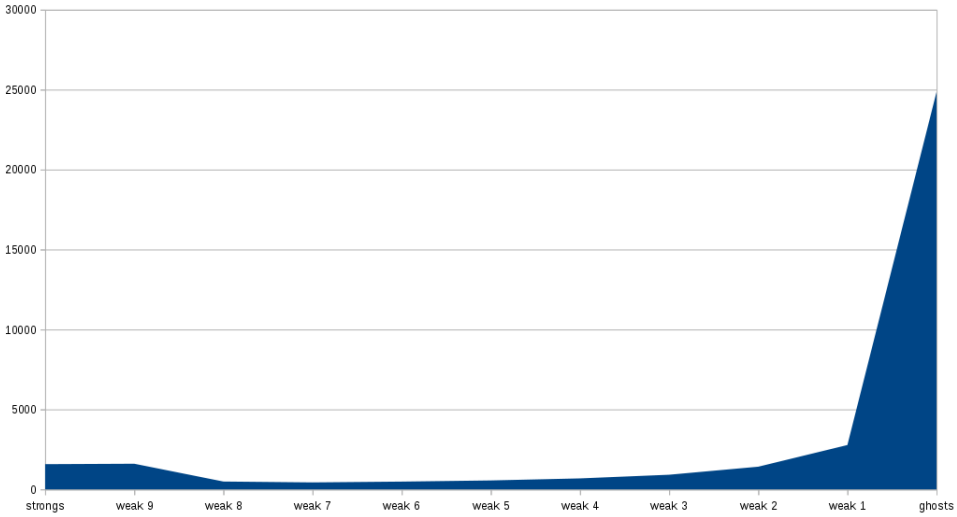

Fig. 2: Distribution of strong, weak and ghost nodes from a sample of 1317 'snapshots' of the network from the last week of 2014

A glimpse of an Extended Bitcoin Ecosystem

Gathered and distilled data on the distribution of the nodes can be geographically displayed through the CartoDB[50] platform. A map of the small sample (fig. 3) shows a highly-distributed ghost population, probably composed of recurrent users or curious bystanders of the network. Among the weak distribution, the majority are part of the weaker, which means that most probably

50 © OpenStreetMap contributors © CartoDB attribution (https://cartodb.com/)

are not part of dedicated servers, but eventual users of the Bitcoin Core, who, for example, connect to the network just to make a transaction but without the intention to continually preserve its infrastructure[51]. It is feasible to argue that a significant number of ghost and weak nodes are zombie machines, especially in geographic areas where low-cost bots are common (Levchenko et al. 2014). Strong nodes, on the other hand are scarce but solid. Given the range of time and schedule of the sample, it is highly unlikely that they have unwilling operators. These nodes have been connected uninterruptedly, and thus are, for whichever reasons, resolute supporters of the network. It is reasonable to assume that many strong nodes are miners and thus benefit economically from their role.

It can be observed (fig. 3)[52] that weak and ghosts usually encircle the strong regions: providing a map of interest where urban areas produce stronger nodes, encircled predominately by less interested parties in concentric rural areas. For example, London is clearly a comfortable niche for strong nodes, and its surrounding suburban areas are populated with weak and ghost nodes. Therefore, showing an urban and highly localised community of network upholders, and a stronger commitment to the network situated in the north of Europe. A point of departure to have a rational reading of the map must obviously consider that a great percentage of blank areas (e.g. Russia) are not inhabited or do not have distributed Internet access. Therefore, blank rural areas and highlighted urban centres are expected.

51 As far as I know, there is no way to know if a node is the public interface of more than one machine, e.g. a mining rig. Also, nodes may also be hijacked computers, as this is a common practice both inside and outside the bitcoin network (Litke and Stewart 2014; Levchenko et al. 2014), and evidently should not be considered as strong supporters. However, there is no guaranteed way to identify hijacked nodes, due to Bitcoin protocol restrictions.

52 This map can be thoroughly explored at: https://timeknows.cartodb.com/viz/7b8e0d76-edb2-11e4-a3b1-0e43f3deba5a/embed_map

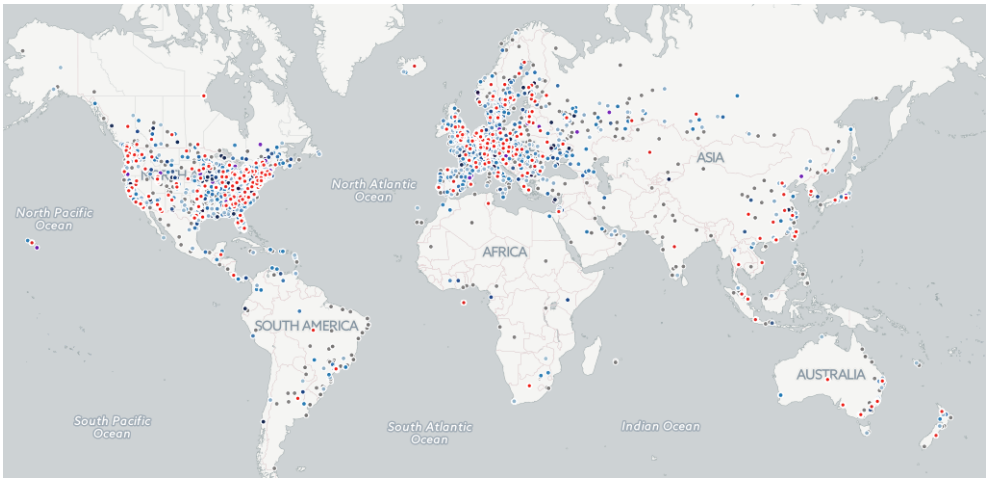

Fig. 3: Map of strong (red), weak (blues) and ghost (grey) nodes from a random sample of 15 'moments' of the network between March and May 2015.

In their great majority, strong nodes inhabit USA and the north of Europe, and in a minor scale, the east cost of Asia. The bitcoin network replicates the centrality behaviour of the Internet: the US has also been identified as the core country in the hyperlinked network (Barnett and Sung 2005, 226), after examining clusters of communication in top-level country code domain names (ccTLD). Also, 10 of the 13 Internet DNS (Domain Name Servers) root servers are located in the US, while the other three are in Sweden, the UK and Japan (on this, Rogers notices how the Internet has always been geographical by design [Rogers 2013, 41]). DNS[53] leverage on control and power within the Internet has had its own share of controversy (Goldsmith and Wu 2008, chap. 3). DNS play an important role for the bitcoin traffic, if only for the first run of a node in the bitcoin network[54]; and all its communications rely on TCP (Transport Control Protocol), most probably routing over the US like a lot of the digital traffic. US infrastructure centrality is also reflected on the organisations where the Bitcoin network moves. This proves that the global network is in reality a very localised phenomenon, with a fistful of nodes in Latin America, Africa and the Middle East. A closer regional look (figs. 4, 5, and 6) shows that most of the strong nodes in Europe belong to the UK, Germany, France and the Netherlands, but again, few can be considered committed in Spain, Portugal and the whole region of the Balkans. It shows that

53 The Domain Name System servers are in charge of translating machine-readable internet addresses (e.g. www.google.com) to Internet Protocol addresses (e.g. 216.58.206.142). They work as a directory and reroute traffic according to the domains and subdomains of the address.

54 Interestingly, the first fork of the Bitcoin protocol was Namecoin, a cryptocurrency which serves as an alternative decentralised DNS.

unlike other emerging payment and value storage systems like M-pesa (Jack and Suri 2011), Bitcoin is a phenomenon, whose network support resides in the north. This distribution replicates and reinforces the so-called Digital Divide Cartogram (Lovink and Zehle 2005, 110–11), which depicts a map where countries sizes are inversely proportional to their Internet usage, showing a world bloated on the south (with some exceptions). Updated maps that also consider the proportion of Internet users show that this digital divide remains (Stephens 2012). It is not surprising that regions with a high number of Internet users are also hosts of many strong nodes. However, it is interesting to see that regions with a great percentage of Internet Users are not necessarily the ones with the biggest percentage of strong nodes (Fig. 7).[55] Canada, the Czech Republic, Australia, France, Germany, Ireland, the Netherlands, Singapore, Sweden and Switzerland show a considerable number of network users when considering its population of Internet users.

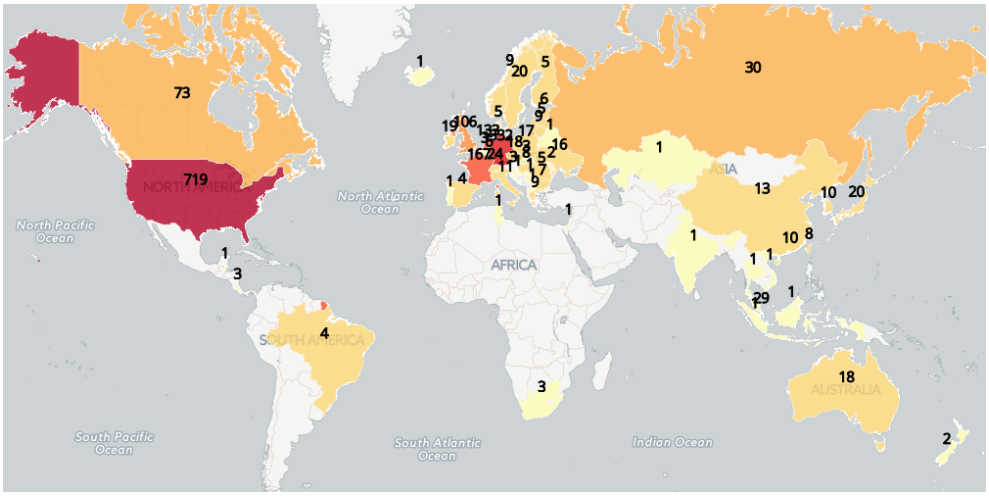

Fig. 4: Strong nodes in the world

55 Internet Live Statistics ranks the total number of Internet users by country based on statistical analysis from different sources: the International Telecommunication Union 2015, the World Bank Group, the CIA's World Factbook, and the UN Department of Economic and Social Affairs (Internet Live Statistics, 2015).

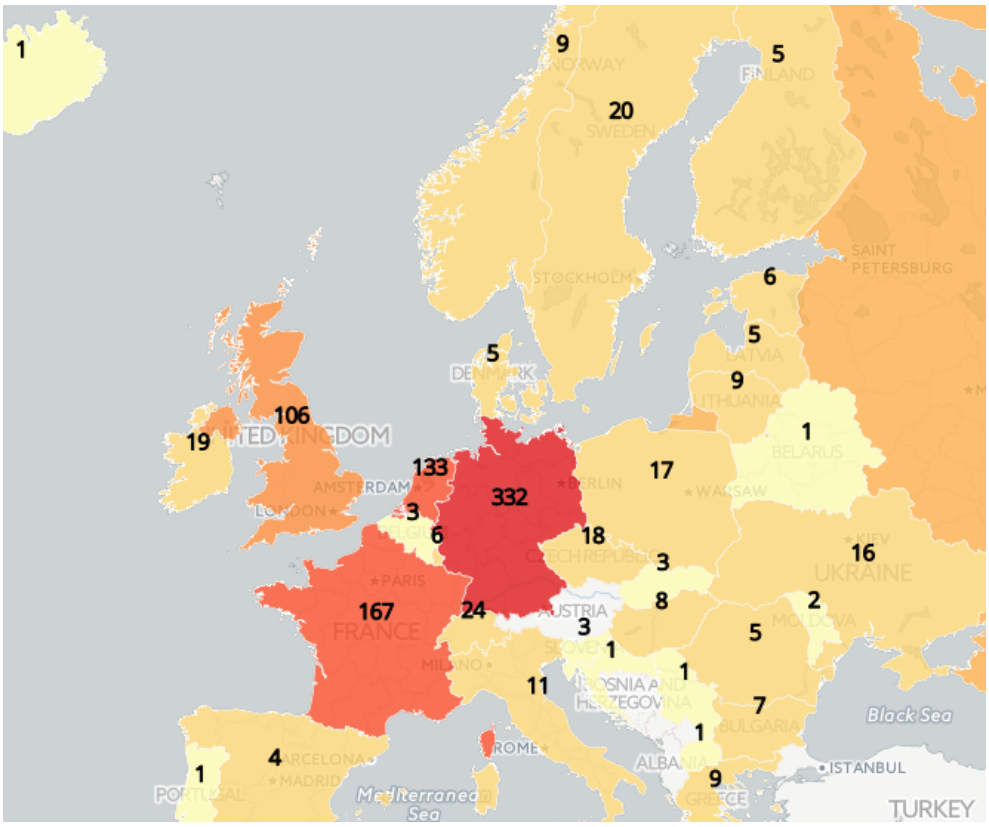

Fig. 5: Strong nodes in Europe

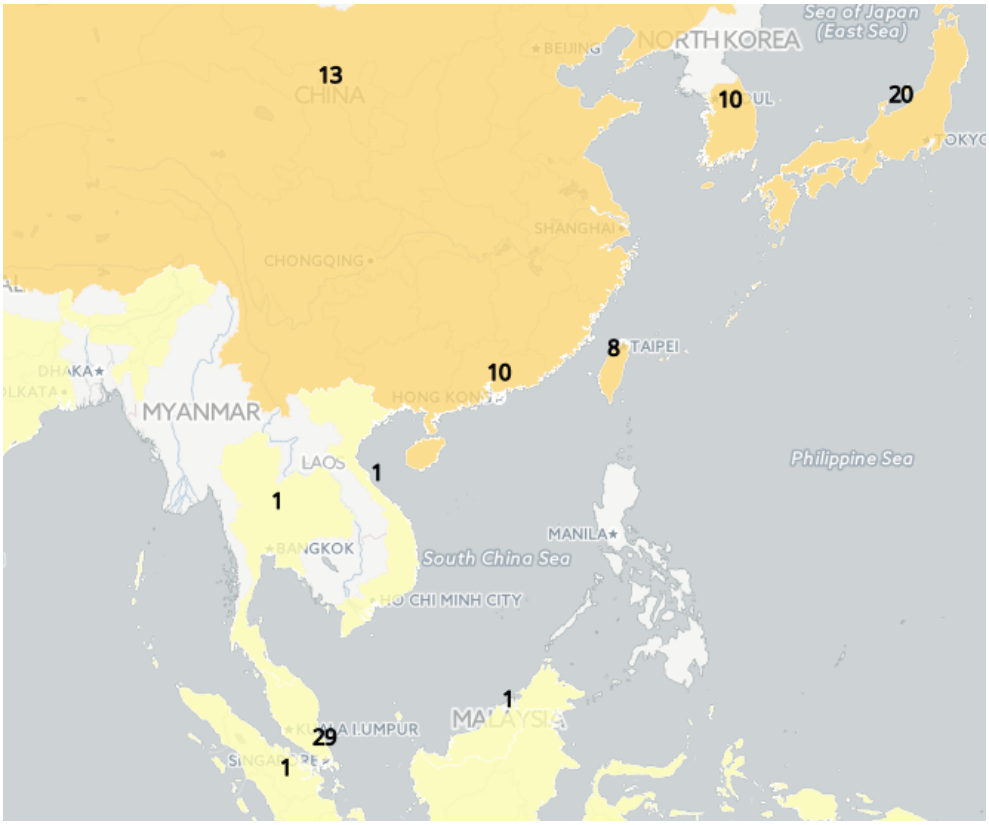

Fig. 6: Strong nodes in Asia

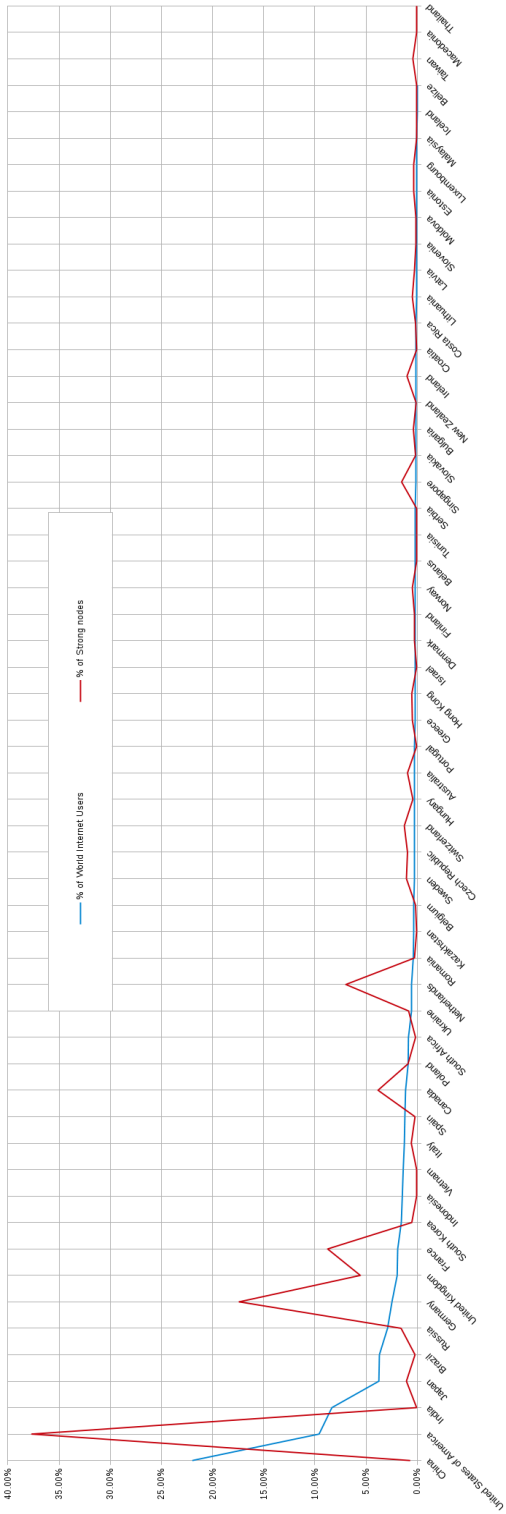

Fig. 7: Percentage (in red) of strong nodes and percentage (in blue) of Internet users (ILS), by country.

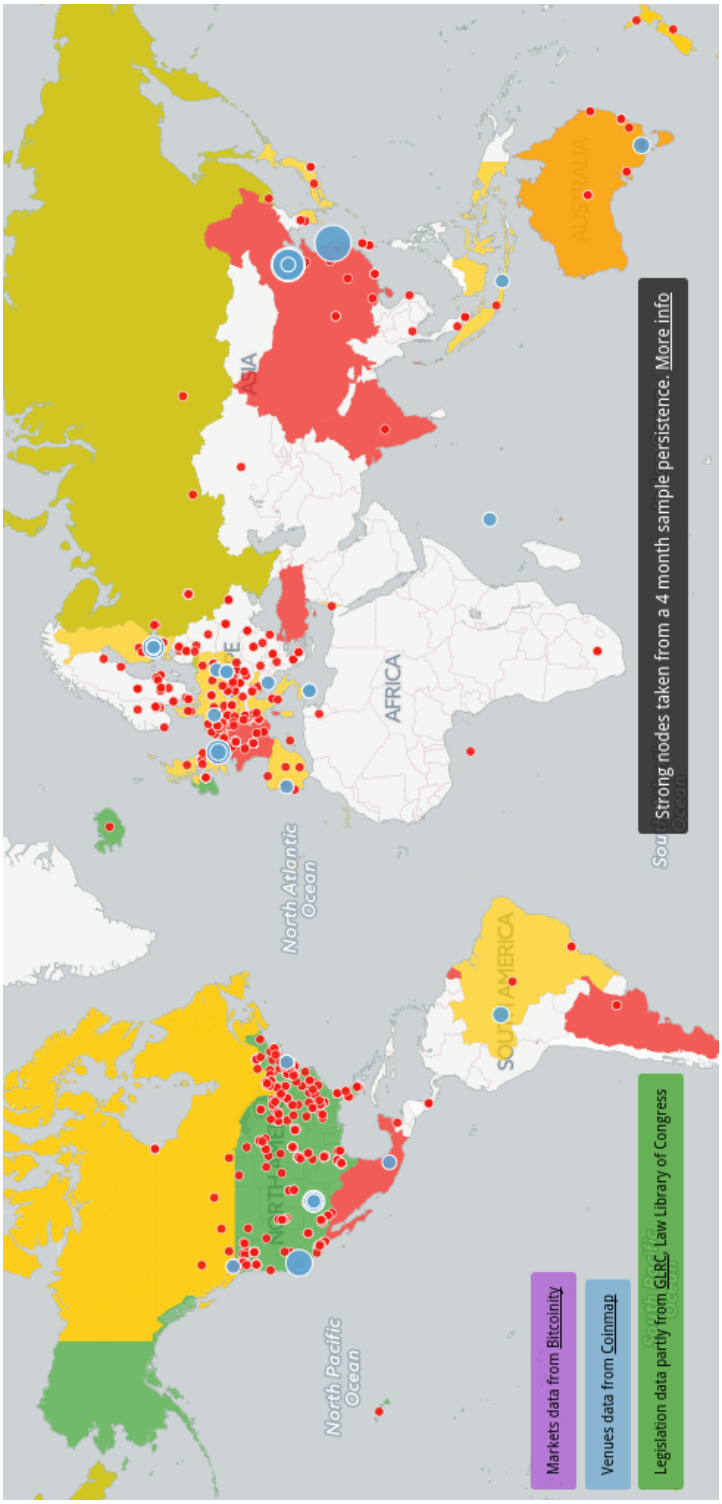

Fig. 8: Geography of a Bitcoin Ecosystem, including country legislation status on Bitcoin (restrictive in red, cautious in yellow, and permissive green tones), strong nodes (red points), markets (blue points, sized by market share)

Separate retrieval and distillation processes of the data generated by the network allowed me to display a visual ecosystem of bitcoin related agencies. The resultant map shows expected behaviour of the ecosystem, for example, a high number of strong nodes and buoyant markets inside permissive/cautious legislation niches. But it is in the discontinuities of the stacked agencies where it is possible to observe the socio-technical guts of the system. Following the fractures, China becomes evidently the most interesting location in the map: considering its huge number of Internet users, it has a noticeably low percentage of strong nodes. To this it adds up the outstanding share of the market it has in relation to exchanges headquarters (fig. 9).

China is one of the few countries that has enacted harsh regulations on cryptocurrencies. At the end of 2013 it classified Bitcoin as a “virtual good” and forbid financial or payment companies to deal with it. It also prohibited third-party payment processors to deal with cryptocurrencies exchanges. Just a few months before, Baidu, the search engine Chinese giant, announced it would accept bitcoins (‘Chinese Internet Giant Baidu Starts Accepting Bitcoin’ 2013). A few days after the announcement, the 'Chinese google' stopped accepting it (‘Baidu and China Telecom Stop Accepting Bitcoin, Price Slumps Again’ 2013). After this, BTCChina stopped accepting deposits in Yuan. Almost a year later, at the end of January 2014, it was accepting the currency again. In March of the same year, it was reported that some banks effectively shut down some Bitcoin exchanges accounts. But despite the discouraging legal environment and the minimal number of committed nodes, Chines exchanges accumulate the majority of bitcoin stockpile. This remarkably unbalanced situation depicts the existence of a second indicator within the network other than the sum of nodes, that is, not so much the quantity, but the node quality. In theory, every node replicates transactions and works to build blocks of them, therefore producing bitcoin units[56], but in practice, only a few nodes have the capacity to produce bitcoins. These nodes can be considered actual miners, who use dedicated hardware for the operation, and usually associate in pools due to the amount of computer power needed to successfully produce new units. Estimations of these pools' capacity of production —or hashrate within the Blockhain— show (fig. 10), again, that a handful of pools

56 There is a 'reward' of 25 Bitcoins per valid block construction, which is the only possible way to produce them.

operate the majority of the blocks. What is more, three of the biggest pools, BTCChina, Antpool, and F2pool are operated from China.

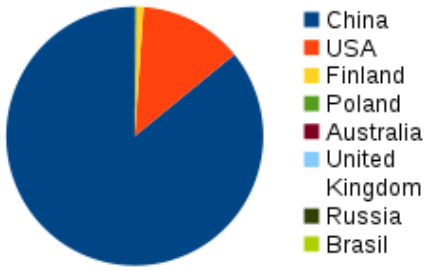

Fig. 9: Location of headquarters by market share

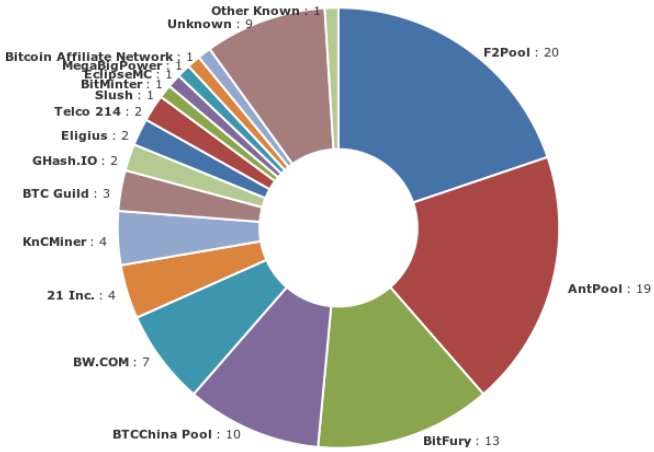

Fig. 10: Percentage of mining pools hashrate distribution from June 18 to June 22, 2015 (screenshot from https://blockchain.info/pools)

The previous analysis of the map leads to a more readable image on the weight of the Chinese territory for Bitcoin. Neither nodes, nor miners or markets are by themselves representations of China as a nation, however, they do represent a crucial agglutination in the Bitcoin ecosystem space. The analysis also shows an unequal distribution that is unique of this digital object, that of the production as computer power and distribution as currency exchange. Other significant findings may be found by zooming into other zones of the stacked map layers.

This section made evident two different kinds of limits: one regarding the network, and the other regarding the method that mapped it. First, the limits or boundaries of the backbone geography of the bitcoin network. Nodes can be traced with a considerable amount of exactitude to show that, for example, despite being present in 138 countries there is not a single node in Mali, the 40th country in the world by means of Internet users. A clear material map of the machines running the network can be charted. Any alleged immateriality is underpinned by the fact that exactly one computer in St. Lucia, belonging to a user who willingly decided to try the Bitcoin-core software, helped to build Bitcoin's existence, by packing information transactions that travelled through the pipes of a telecommunication company. It is for sure challenging to trace a world map when a 'universal' network centralises itself in five countries. Vitai Gupta, a Bitcoin enthusiast and critic, stresses the need to develop the use of the cryptocurrency in developing countries, where it has the possibility to be a social meaningful transformation and not an extension of capitalism ideologists (*CoinScrum and Proof of Work: Tools for the Future* 2014). This technical approach speaks only for machines connected to a network and shows that the network takes place, as an aggregated material medium, in specific location, and is non-existent in others, thus, is subject to geographical limits.

The second kind of limit is that using a technical and geographical approach to understand the particular notion of space in cryptocurrencies does offer some insights on how the network operates technically, and an interesting idea of its associated geographical territory, but certainly a 'limited' notion for making sense of a comprehensive space that goes beyond the infrastructural. It is

not possible to build a political geography from just this kind of territorial networks. Some important actors and relations remain unidentified. The tracking of the physical network does show that cryptocurrencies are phenomena played in countries not directly correlated with their Internet inclination, it hints to communities of interest within certain countries but says nothing on these places' policies on the subject. Nor can the complex relations between the actors be addressed by just looking at the behaviour of physical networks. Thus, the next section adds political concepts that shed light on how to understand the relation of the blockchain with other actors. As in previous chapters, I pay particular attention to the relationship with traditional authoritarian structures (i.e. the state) and with private platform services, since public blockchains can be thought in between the two: they exploit the non-territorial arrangements of the latter, but try to partially replace the authority model of the former. The matter is then directed towards a question of the digital sovereignty of a non-territorial space.

4.3 Non-westphalian Authorities

Digital Method researcher Richard Rogers' road of the Internet, after its hyperspaced and spherical momentum, proceeds to networks. His classification not only offers adequate methodologies for research, it also acts as a map for possibilities of movement, and in this context, of the creation of different 'space arrangements' or 'topologies' (Rogers 2013, 40). Vectors towards localisation of centres in an unmapped space *via* links, delimitation of discussion zones and discursive possibilities *in* spheres, and finally, continuity of controversies *through* networks. The kind of space that is created by network movement is more suitable for the displacement of the bitcoin network and the layered complexity of its actors than any territorial approach. Topology has been identified (Lury and Wakeford 2012b) as an order of spatial and temporal continuity within cultural, economic and political forms of cultural life. On this reading, topological objects are not identified based on a structure of fixed or essential properties. On the contrary, the space is mapped according to its fluidity. Transformations are tracked as continuity and in doing so a space is charted, not by a previous order of time and space. Here I follow the idea that there exists a tendency towards the

topological in culture practices: “Culture is increasingly organized in terms of its capacities for change: tendencies for innovation, for inclusion and exclusion, for expression emerge (...) as a field of connectedness, that is, of ordering by means of continuity, and not as a structure based on essential properties” (Lury and Wakeford 2012a, 5). These practices are clearly expressed in the political and economic world in the form of socio-technical activities of sorting, calculating, listing, ranking and in general in the establishment of relations by quantitative comparison or measurement. As I have developed in the first chapter, the strategies of control of the distributed political framework of the Empire brings new notions of authority and sovereignty, reflected and enhanced in digital phenomena like the blockchains. The space were blockchains dwell is too imbued with a notion of sovereignty provided through its topological performance, and marked by an implicit confrontation with the territorially-based restrictions of the state.

Hardt and Negri identify money as the means of control of the Empire that holds together aristocratic power. The Empire narrative also argues that distinct powers are associated with different means of control: the monarchic or absolute power relies on the *bomb* as an executive capacity of destruction; the aristocratic power relies on *money* as a tool to redistribute national monetary structures towards commercial entities, highly concentrated in financial centres; and finally, the democratic power uses *ether* to articulate sovereignty through communication systems, to subordinate society to communication (Hardt and Negri 2001, 347). It is precisely money and ether[57] (information) that gets conflated with the emergence of the blockchain. While the current finance system factually merged these two aspects of control —money exists primarily in the form of alteration of, and communication between, financial databases— the blockchain does it in a novel manner. As I will argue in this section, it de-territorializes and re-territorializes[58] the state role on the creation and communication of money: it diminishes the relevance of geographical territories and jurisdictions, and at the

57 Curiously, the token in Ethereum, the most developed blockchain with programmable capabilities (i.e. “smart contracts”) is also called ether.

58 Although inspired by Deleuze and Guattari concept of de-territorialization (Deleuze et al. 2009), I am not following their work. My use of territorialization is simpler: it denotes on one side a lack of importance regarding earth topographies (de-territorialization), and on the other the attempt to expropriate state functions on the production and transmission of assets (re-territorialization).

same time moves the organisational and instrumental means of production to a different notion of space.

De-territorialization: Technological Zones

Although blockchains are traceable, they are able to sidestep the necessity for geographical financial centres of the aristocratic power that Hardt and Negri identify. The clusters do exist, but in a different order. The previous section located the registered headquarters of the crypto-market exchanges in 2015, and found that while examples like Coinjar, which fled Australia to seek the financial freedom provided by the UK, a substantial majority of exchanges and mining industries clustered in Chinese territory, despite the harsh regulation against crypto-markets.[59] This de-territorialization that the blockchains are capable, minimises the subjection towards states. The surface where the two meet (blockchain-based projects and state regulations) is not immediate, as states have no direct effects on the governance or development of the blockchain (see Chapter Five for the case of Bitcoin development).

The mediation between blockchains as a network technology, and states as normative jurisdictions is closer to what has been called a technological zone (Barry 2001; Barry 2006), which preserves a topological landscape, since this communication layer is understood in spatial terms. Barry identifies three kinds of technological zones: metrological (common forms of measurements), infrastructural (common connection standards) and zones of qualification (practices assessed by common standards). These zones are defined as "a space within which differences between technical parties, procedures and forms, have been reduced, or common standards have been established." (Barry 2006, 239). They work as buffer zones, and are relevant for this discussion because they are characterised for being neither "territorially bounded nor global in their extension" (Barry 2006, 209) but still of political and economic significance. These kinds of buffer zones are being consolidated between the legal realm and the financial side of the network. They are more likely encouraged and developed by

59 This remarkable situation remains: in September 2017 the Central Bank of China banned Initial Crypto Offerings (ICO) funding (the blockchain version of IPO's), however, the Chinese miners and crypto-markets are still a considerable majority in the blockchains ecosystem.

state managed financial institutions in the face of a possible widespread use of cryptocurrencies, or, perhaps more probable, sporadic misuses of them.

An example of this standardisation process is the *Bitlicense*, issued by the New York State Department of Financial Services to regulate the business use of cryptocurrencies since 2015('NY Financial Regulator Lawsky Releases Final BitLicense Rules for Bitcoin Firms - WSJ' n.d.). The license allows Bitcoin related companies to store, buy, sell, and administer cryptocurrencies. As of January 2017, only three licenses had been granted, and the new regulation forced companies to relocate (e.g. Bitfinex, and Kraken) (Roberts n.d.). Like with the Chinese government restrictions, the Bitlicense resulted in the relocation of some business headquarters, but did not affect the overall development of Bitcoin, which keeps gradually expanding.

Another way to measure the limited effects of regulation on the performance of the system or overall adoption is to observe the market price of Bitcoin as a regulatory position is declared by countries. Bitcoin represents a particular challenge for regulation, since even though the hovering activities associated with the currency can be controlled through traditional disciplinary methods, such as the Bitlicense, the coin itself was designed to be resilient in this sense, since it is relatively easy to use it through communication channels (e.g. a VPN tunnel, or even through the TOR network) despite a formal prohibition. As an example of this dissociation, I tracked formal statements of different countries[60] regarding digital currencies (not only bitcoin, although it is the most used example) to observe if there was a direct correlation with the coin price fluctuation. Most reactions cluster in the range between October and December 2013, unsurprisingly, this is the moment when the price achieved a record peak (1151 USD on the 4th of November) up until 2017, and attracted mainstream attention. In the statements' dataset, few countries have taken formal legal measures: of 43 countries, only Australia, Brazil, China, Germany and New Zealand have adopted explicit legal responses and from these countries, only China has forbidden its use in some manner. Most states are rather cautious, strongly advising precaution on the use of digital currencies but without necessarily

60 Most of this information, so far, comes from the Global Legal Research Directorate (2014). However, a site dedicated to tracking cryptocurrencies legality around the world, with considerable additions can be found at http://bitlegal.io/. These rankings do not always agree with my own classification.

expressing a negative opinion. This restrained may be tied to the incapacity to adapt the cryptocurrencies definition to one within the previous legal enclosure of fiat currencies. Fig. 11 shows changes in price a day before and a day after a resolution by countries. In it, colour represents reception of alternative digital currencies: red is a strong negative, green a strong positive and blue a neutral or mixed one. I have included only countries where a legal declaration has been made. For instance, a press release of the Bank of Portugal declares, based on a study of European Central Bank that "users can buy and sell virtual currency with legal tender and purchase goods and services in the real and virtual world" (The Law Library of Congress 2016).

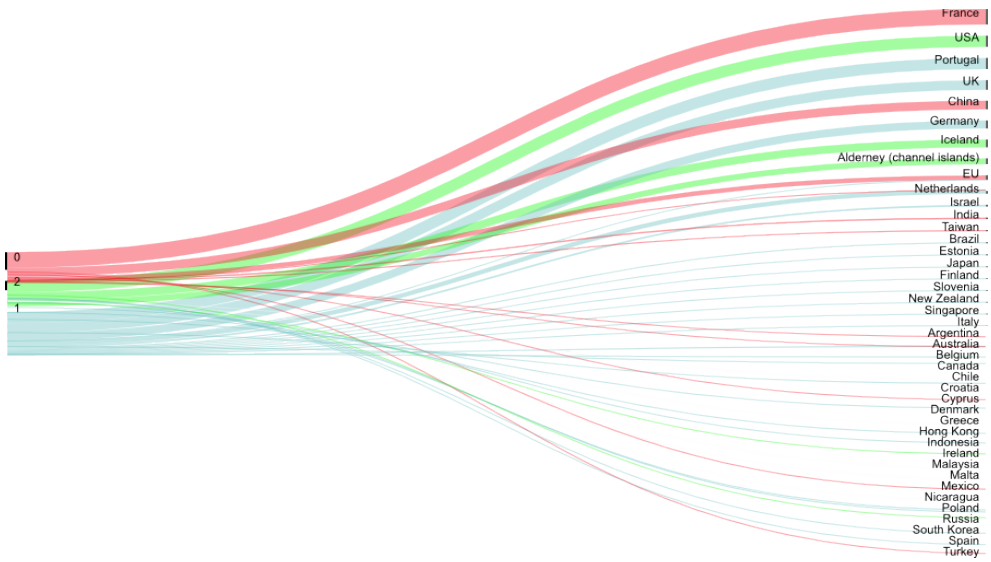

Fig. 11: Resolution of countries by Bitcoin price change

The biggest upscale coincides with the negative response of France, followed by the positive resolution of the U.S. and the neutral effect of Portugal. This apparently shows that the rise of the price was barely related with the position of any government. Nevertheless, the attention of the media and governments on bitcoin at the end of 2013 most probably corresponds with the rise in price and popularity, regardless of whether the state actors had a neutral, negative or positive response to the phenomenon. There are uncountable variables involved in the market fluctuations of the value, but it is reasonable to expect that a negative assessment by a normative authority representing a

country would have a more palpable effect on valuation than what is indicated in the data. However, what I claim is that while the system is affected by territorial authorities, its valuation, development, and expansion is not subjected to them in the same way that fiat or even alternative currencies.

Relations between state, law and financial institutions, and a new decentralised transfer system based on cryptography in a public ledger, are the emergence of a metrological zone. Institutionalised entities certainly deal with a recent and confuse device, and look for a language to measure or adapt it to existing legislation. Barry's concept of technological zones also offer the advantage of being localised despite its geographical distribution, i.e. a zone formed by a set of different laboratories working on the same topic "is not confined to any particular nation or region; but rather it is nonetheless, strongly tied to specific institutions, persons and devices which have been the object of huge technical and financial investments" (Barry 2001, 52). The zone is defined more by its converging points than its territories, thus, actors can be quite localised despite geographical or border dispersion. These also include human and non-human elements. I previously stated that the Bitcoin network is made of communities not directly associated with state policies. And although Bitcoin's functionality is not defined by territoriality, its daily operation does depend on the administrative power set by political territories. The price roller-coaster was not defined by the legal position of key countries, but the price peak may be what alerted governments to begin paying attention to cryptocurrencies as a possible threat to the control of capital circulation. This forces them to take a stand on the subject that does have an influence on the Bitcoin space metamorphosis. The UK still represents a niche for autonomous and to a certain point unregulated development of cryptocurrencies, but that is temporary and most probably will be modified based on the proliferation of the technology as a currency. Australia, on the other hand, is prematurely developing a qualification zone where standards on the legal and the financial are set and assessed between un-territorialized technical parties and state institutions. Bitcoin remains a distributed digital network outside Australia, but some of the actors of its space become overlapped in this buffered zone and have to settle on it or, like Coinjar, have been forced to emigrate.

These buffered zones are useful to explain the agreements between an emerging topological phenomenon, the blockchain as cryptocurrency, and established topographical authorities. However, the second kind of relation with territorial arrangements, the re-territorialization, considers the aspects of this relation that are better described by competition than agreement. The following final section provides a theoretical framework to think about blockchain technology as a space that is part of a new kind of sovereignty among the digital.

Re-territorialization: Digital Assemblages and Stack Sovereignty

Barry's technological zones are not necessarily to be conceived as a form of social structure, but an abstraction capable of making visible a particular social scenery while contributing to the visibility of its spatial forms. While the concept is particularly useful to think about the role of standarisation processes between two entities, it is less concerned with authority conflicts between the parts. Sassen (2006) uses the term 'imbrication' to talk about a particular kind of relation between digital and non-digital entities that takes into account power leverage in the affiliation. Imbrications function as assemblages that shape 'a particular kind of territoriality' (Sassen 2006, 326), through an interdependence of digital and non-digital devices. This dependence, Sassen argues, does not make them hybrids or irreducible to each other. Nowadays digital markets and political actors do rely on each other for their development: infrastructure for the digital markets is constructed via nations' allowances and private investment, day-to-day functioning is also funded by private networks, states benefit from the efficiency of these markets to trade goods and money in all its forms. Within Sassen's argumentation, an imbrication is created here between two finance entities: a 'supranational electronic market space', which is 'spaceless' in the sense that it is decentralized and therefore not necessarily geolocated; and a financial centre space, subject to national law. The second is the nationally embedded part of the first. The digital and non-digital imbrication between these two spaces act as a power leverage between global markets and nation-states authority. It consists “of both the use of that authority for the implementation of regulations and laws that respond to the interests of global finance, and the renewed weight of that authority through the ongoing need for financial centres” (Sassen 2006, 338).

Sassen also notes that some new technologies create 'networked assemblages', that enable new kind of political actors, who by generating particular forms of power build in part the new assemblages. Global capital markets, as stated before, gain the power to discipline states by guiding territorial economic policies. It also strengthened older actors, like trading institutions and corporations, but what draws Sassen's attention is that the new actors are "capable of engaging the competence, scope, and exclusivity of state authority" (Sassen 2006, 328). Sassen also notices that in the case of global markets, digitalisation is more a tool than a mastermind, regardless of the importance of technology, the outcome of new forces is driven by finance and not a distinctly digital logic. That is, it is the finance models that feed the logic of assemblages such as the derivatives and securities markets, and these happen to be digital.

While many of the examples and uses of Blockchain technology are strongly compatible with finance, I argue in the first chapter that a computational paradigm drives the main reformulations brought by distributed production. The case of Bitcoin is a good example, since the technology and network are not part of a private corporation. Its main elements are underpinned by the banners of openness and common infrastructures, themselves ideals of the open software world. This does not mean that private financial entities are stranger to the technology, and in fact much of the latest blockchain development, like other open software examples, is nurtured by the attempts to integrate this technology to the ends of the private financial worlds. So, while blockchains are networked assemblages grounded on a computational paradigm, they generate via their particular distributed production process, their own powerful actors, like miners and markets, who benefit financial logic and engage in a competition with state authorities. The "computational paradigm" is both the automatised production of unique assets in a distributed network (analysed in the first chapter) and a claim of a new non-territorial space.

The claims for space, state competition, and markets empowerment merge in the idea of "open", as read by Hardt and Negri. One of the main characteristics of the Empire is to portray itself as an open non-place: "Perhaps the fundamental characteristic of imperial sovereignty is that 'its space is always open' (...) the modern sovereignty that developed in Europe from the sixteenth century onward conceived space as bounded, and its boundaries were always

policed by the sovereign administration. Modern sovereignty resides precisely on the limit. In the imperial conception, by contrast, power finds the logic of its order always renewed and always re-created in expansion" (Hardt and Negri 2001, 176). Very much like in the early Roman Empire, the spaceless utopia brought by digital communications and extended on blockchains, the openness where it dwells is based on a *frontierless* expansion, *imperium sine fine*. Like the cyberspace imaginary that is always in becoming, which was sold "as an endless space for individualism and/or capitalism, as an endless freedom frontier" (Chun 2008, 43), the blockchain space for stateless exchange is utopic for finance markets. It is the ideal machine inasmuch as it maintains the idea that it has no outside, unlike the spaces of modernity "thwarted by barriers and exclusions; it thrives instead by including always more within its sphere" (Hardt and Negri 2001, 190). The disappearance of the territory as a technology of power associated with the modern state, is the mirror image of the promise of frictionless circulation for markets. The blockchain is then both a spatial and a political economy claim.

Perhaps these dual characteristic is best reflected in the profound role cryptocurrencies play in the dark market. The illegal digital communities gathered around projects like the Silk Road, and most recently Alphabay grew with the use of cryptocurrencies (Bitcoin, in particular). The markets challenge at the same time the territorial jurisdiction and the normativity of the state and capitalise on free circulation, by using cryptocoins in deep spaces of the internet. Arguably, these two examples were located, seized, and the minds behind them where judged as any other criminal activity performers. However, while they were online, they exploited the capacity of blockchain technology to challenge state regulation to circulate assets in a non-territorial space. Also, while these two markets were halted, many others sprouted in their absence.

These kinds of markets can efficiently function in great part due to the re-territorialising effect of blockchain technology. By this I mean the attempt to absorb the state functions of currency regulation of production and exchange. The distributed, non-human trusted network automatises the production process to predefined rules, regulates the efficient movement between parties with mathematical certitude, and allows itself to be publicly audited. Even considering the human factor involved in the development and decision-making of its design,

the machinery does remain a clever partial substitution for a very basic money control emulation of modern state scheme of monetary production.

The importance of the computational factor and the generation of a non-territorial space is better integrated with Benjamin Bratton's stack model. Posited as a novel political geography framework, the Stack is also a reaction to the constrains of utopia (pre-2008) and dystopia (post-2008) readings of computing systems: "we need new and better models, because computation already operates in ways that have surpassed and overflowed the regular cartographies" (Bratton 2016, xviii). Computation is understood not (only) as machinery, but as a planetary scale infrastructure, not a technology inside a society, but a technological totality where the social is built. As mentioned at the beginning of this chapter, Bratton identifies the modern Westphalian notion of space, the nation-state, as core jurisdiction, as a design of geopolitics that is the result of planar geography, of a process of "separating and containing sovereign domains as discrete adjacent units among a line and horizontal surface" (Bratton 2016, 5). The Stack, however, disregards the planar and presents space as a series of interconnected non-geographical layers, capable of reconfiguration. Within the Stack, the states as an authority element do not so much decline, as much as their condition "is qualified both by a debordering perforation and liquefaction of this system's ability to maintain a monopoly on political geography, and by an overbordering manifest as an unaccountable proliferation of new lines, endogenous frames, anomalous segments, medieval returns, informatic interiors, ecological externalities, megacity states, and more" (Bratton 2016, 6). It would be perhaps more adequate to say that the state is overflowed by the complexity, velocity, and interconnection of elements performing in a planetary-state computation model.[61] The Stack conflates governance and non-territorial space: it is not a representation of the state, or a reformulation of the state in terms of a machine nor vice versa: Bratton asserts that machines are governance, the Stack *is* the machine *as a* state.

The way sovereignty is enforced in this non-planar space is through the control of the *borders*. The Stack is the accumulation of systems nested into other systems. This multiplies the boundaries instead of vanishing them. Sovereignty is

61 One of the main examples of Bratton on the indigenous governance of the Stack is Google, which is defined as a "nonstate actor operating with the force of a state but unlike modern states, it is not defined by a single specific territorial contiguity" (Bratton 2016, 10).

what draws a line between what each system allows, and through software these gateways are automatised (SCI-Arc Channel 2016). Unlike the Westphalian space, these lines are not fixed and are in constant mutation, and are even reversible: "Unrestricted by the brakes of the proper *nomos*, the absolute motivation for capture extends up and down from molecular to atmospheric scales", but not untethered, as "they congeal layer by layer into a metastructural order of a different governing order: a machine that is a state held together by deciding the spaces of technical exceptions as much as legal ones" (Bratton 2016, 34). The decision on the exceptions, on what belongs and can be integrated into the system is automatised.

Blockchains fit the stack model. Its core functionality does not require a geographic map, and they supply state ordering with automation. They are a material stratum, and subject of location, but they participate in a different ordering. While I showed that there is a bidirectional influence between nation-states and corporations, and cryptocurrencies, the relation is, from the point of view of the blockchain system, circumstantial and re-placeable. The state exists, and interacts with the blockchain in technological zones and networked assemblages, both as regulatory nemesis and enabler of jurisdictional headquarters, it interpellates the blockchain. However, states are non-essential for the performance of blockchains. The Stack generates its own subjects and authority models, based on machines, which, like the blockchain act as automated "decision-making interfaces" (Bratton 2016, 32). The interaction with the state is not in the terms of subjection. The Stack's sovereign and space model does not depend on territorial arrangements, even thought it is in a constant relation with them.

The design of the interface, however, is not technologically determined. Despite heavily outsourcing the control of its borders to the machine's own logic presented in Chapter One, the general design of this outsourcing happens within affectively and ideologically charged human-led governance developments. The final chapter will observe part of this decision-making actions in Bitcoin, as a case study to show the non-deterministic side of the inner working of blockchain technology.

Chapter 5: Strategies for Governance and Bitcoin's Scaling Controversy

I have previously shown the prehistory or techno-political lines of descent that gather in the emergence of Bitcoin (Chapter Three), and the predominance of an algorithmic logic in the production and exchange of its assets (Chapter One). The discussion on the mapping of its network (Chapter Four) also angled toward the computational aspects of the system, in particular in relation with the governance of territorially-based institutions. However, Chapter Four also considered the important, though dispensable, relation between the non-westphalian network of the blockchain and the normative and disciplinary institutions of the state. In this chapter, I expand on the non-computational elements that build the blockchain, by observing the influence of the governance processes in the design of the Bitcoin system. In a way it can be read as a counterweight to the first chapter, but actually it is more a complementary argument, insofar as it connects the governance and organizational process of production of a software/protocol with its outcome, itself a system oriented towards the non-human production (of assets), control of communications, and even novel governance models.

This chapter depicts strategies for governance in the development of Bitcoin, and their successes and failures, discerned through the analysis of one controversy (block-scaling), a protracted issue among the Bitcoin community: developers, miners, cryptocurrency exchanges, stakeholders, and enthusiasts. I follow the discussion exclusively among the main developers, from 2013 to one of its more critical points in 2015, and pay particular attention to two confronted spokespersons (Mike Hearn and Peter Todd). I distinguish between three topics that are usually mixed in the general controversy discussion, but are not interchangeable: scaling the capacity of the blockchain, enhancing the size of the blocks, and producing a hard-fork of the chain. The purpose of this observation is to identify the rationale for the disagreement. I will show that this collision is at its core a contradiction —briefly mentioned in the previous chapter— between the utopic ends of decentralization and free market, of a historical concern of strong multilateral privacy and a frictionless competitive system of exchange.

I will start by commenting on the early discussions of 2013 on block size as a strategy for scaling the network, and how they relate to the consensus-enabled governance of the project development. Then I will add the revitalization of the evolved issues in 2015 that generated the outbreak of the Bitcoin XT fork. A fork is a common strategy within open source software (OSS), that allows to sort out disagreements by generating two (usually competing) software projects from the same original source code. The Bitcoin XT fork made visible the formation of two different forces, with opposing ideas of the reasons and ends of a project like Bitcoin. The failure of forking[62] also signaled a critical difference between previous projects and Bitcoin. Thus, I will also argue that the economic nature of the Bitcoin project repealed, or at the very least reformulated, the forking strategy.

The fourth and final notion of utopia is the imagined governance through other means. In particular, the use of technology to replace the continually failed human interaction to produce agreements, trust, contracts, and compliance between parties. Like the paradox depicted in the first chapter, the utopia arch also signals a tinge of irony here: while the blockchain is posited as an instrument to overcome organizational failures, and even as a solution to broader political issues (i.e the democratic processes monitored by the state), this chapter tells the story of the organizational failure to develop such an instrument in the first place. The words of Gregory Maxwell, a Bitcoin main developer, express this inconsistency: “I think governance is incredibly hard and that the development history of fiat currencies shows that mankind is ill-equip to create a strong and sound system via human governance-- not through lack of trying, but because mankind is fundamentally not cut out for it: there is always some excuse that makes people feel justified in compromising the property rights of some for the benefit of (potentially many) others. Bitcoin was specifically created and promoted to replace that kind of subjectivity with machines, but it can't do it if we go around undermining it” (*minersupportTH*).[63]

62 At the moment of this writing (September 2017) a competing fork similar to Bitcoin XT, “Bitcoin Cash”, finally got implemented but has not replaced the Core chain. I will briefly comment on the status of this fork at the end of this chapter.

63 Many of the references along this chapter are encoded with an abbreviation (e.g. *minersupportTH*) of the thread within a forum. A list of *Abbreviated References* can be found at the end of this chapter.

5.1 Strategies for Consensus

The endeavours to bring together the blockchain and democratic processes are a minority when the gross of financial-related projects is considered. It is nonetheless interesting that the implementation of computational rules for negotiation can be thought for an extended spectrum of governance models. From positions that seek to use it as a tool to replace bureaucratic limitations, thus instrumentalizing a system without any other major changes (i.e. the "Flux Party"); to projects that explore blockchain's affordances to extend the participation in democratic life, thus distancing themselves from representative models (i.e. "D-cent" [Decentralised Citizens ENgagement Technologies project]); to implementations that assume the impossibility of a fair democratic model, thus proposing the use of blockchains as a mean for oligarchic governance and organization.

The Flux Party is not interested in proposing policies or making decisions, but only in enacting what their members vote (Siegel 2016). Their proposal replicates the use of the blockchain as a secure exchange network, but instead of considering the tokens as monetary units, they count them as votes which can be spent, swapped, or traded for every proposed bill. This seamless direct democracy system could presumably be supported by a blockchain, and has the double possibility of being used in a more traditional way (i.e. by offering a vote to a trusted party, expert or representative). On the other hand, D-cent, a program backed by the European Union, is concerned with developing "the next generation of open source, distributed, and privacy-aware tools for direct democracy and economic empowerment"('D-CENT' n.d.). D-cent aims to involve participants into the public sphere by offering a "blockchain toolkit" consisting of complementary currencies governance and decentralised trust management systems, both embodied in the fully usable Freecoin, also based in Bitcoin. The use of blockchains is, however, only one of many tools and platforms. D-cent is a bigger project that seeks to bring together grass-root organizations to expand modern democratic models. Finally, Bitcoinocracy (http://bitcoinocracy.com, now called Vote Bitcoin) is a simple implementation to vote on propositions regarding Bitcoin. In it, the votes are made valid by using a Bitcoin address, this makes them unforgeable, but since the creation of wallets is gratuitous, the weight of the vote

is measured in the quantity that wallet holds. The resulting system allows every argument to be decided by the wealthiest part of the population. On its own Reddit thread the creator (Arsen Gasparyan) justifies the oligarchy set up of its system:

> I am not sure whether democracy exists in real life. Perhaps it is just a show made by the rich for the poor (more capital you control - more power you have over the public opinion and thus voting results). Bitcoinocracy does the same, but in a transparent and verifiable manner, without spending much resources on democratic decorations. I think it is somewhat similar to shareholder voting in the public commercial company. If you don't own a company, why would you decide what is better for its shareholders? More shares you have - higher your influence is ('Bitcoinocracy - an Opensource Project to Facilitate Decentralized Decision Making' 2015).

Bitcoinocracy, the D-cent project, and the Flux party have distinct strategies to improve social policies through Bitcoin-based systems. However, the rationale for the proposals has a similar basis. D-cent assumes that the current (pyramidal) social organization was developed during the industrial age, but stagnated in the information age (Sachy 2015). Likewise, Flux party founder Nathan Spataro stated that representative democracy is a system that bloomed to get rid of monarchies, but is unfitted for our current connected society (Siegel 2016). Although visibly different, these projects argue against outdated decision-making systems, outdistanced by the technology that can reinvent them. For these projects, stagnated governance and decision-making arrangements based on hierarchical, imposed, closed, and centralized procedures are to be replaced with their technically-enabled counterparts.

Bitcoin's ultimate goal was not to design a technical replacement for democracy, although it certainly inspired the previous projects. As the first blockchain, it focused on producing a working shared ledger. While it is explicitly a payment system, and not straightforwardly political, like D-cent and Bitcoinocracy, it shares the ideology of replacing trust-related organizational systems with technology. Returning to Maxwell's quote, "*it was specifically created and promoted to replace that kind [human] of subjectivity with machines*". The following pages focus on how a controversial topic —scaling the capacity of the Bitcoin network—showed the relevance of this very subjectivity in the

construction of such technical system. The technical decision-making for scaling, despite its fail-safe strategies for internal governance, made evident two contrasting political ideologies coexistent in the system.

The controversy was centred on the technical solutions to scale as the number of transactions of the network grew. On the one hand, a fairly simple solution was to enhance the capacity of each block in the chain, which is limited by design to one megabyte of information. I will elaborate on why this *simple* technical tweak generated so much resistance. On the other hand, many strategies to deal with scalability without changing the size of blocks were presented —and generated their own resistances. Some eventually managed to get implemented, but not without dividing the Bitcoin community.

Scalability and Disenchanted Believers

Bitcoin's public life started in 2016 with another story about its counted days as a successful experiment, entitled "A Bitcoin Believer's Crisis of Faith", published by the New York Times (Popper 2016). Stories depicting its failure have been a recurring phenomenon along its evolution. The website "Bitcoin Obituaries"('Bitcoin Obituaries: Following Bitcoin While It Dies and Rises' 2016) lists articles that have declared its death, and according to the site as of September 10th 2017, it has already died 159 times. The title of each obituary cites the original reference alongside with bitcoin's price in USD at the time of the publication, as a symbol to counterbalance or even mock the mournful statement. But unlike the great majority of the listed obituaries, the 2016 New York Times piece was not an analysis made by experts at the outskirts of the Bitcoin ecosystem. This story portrayed the deception and abandonment of Mike Hearn, one of the main developers and early supporters of the cryptocurrency. Hearn received his first email from Satoshi Nakamoto in 2009 (*ActionTH*), and started contributing to Bitcoin code at the end of 2010. He became so passionate about it that he resigned his programmer job at Google to completely dedicate himself to the cryptocurrency's development. However, at the moment of the New York Times piece Hearn had sold all of his bitcoins and declared the whole project a

failed experiment. His support faded to the point of asking why anyone would would care about a payment network that:

- Couldn't move your existing money
- Had wildly unpredictable fees that were high and rising fast
- Allowed buyers to take back already made payments
- suffering from large backlogs and flaky payments
- controlled by China
- in which the companies and people building it were in open civil war (Hearn 2016).[64]

The list of the "disenchanted believer" (Bogdan 2016) combines technical and political disagreements. Alongside the block-scaling controversy, disagreements on technical implementations led to severe political disagreements. While Hearn is not the only manifestation of a discomfort with the decisions made inside Bitcoin's core development, he certainly became a public voice for the block-scaling controversy. Because of his unique role, he is the narrative backbone to unfold it.

Scaling the network is in fact an old debate, which scaled itself as the network was getting closer to its transaction capacity. Mike Hearn started a thread back in March 2013, called "Soft block size limit reached, action required by YOU" urging to pay attention to the soft-limit of the block size. Unlike the hard limit of the Bitcoin blocks, which is unmodifiable without consensual changes to the core, the soft limit can be set by each miner as long as it is below the hard limit (of one megabyte). There are different reasons for having different limits, i.e. smaller blocks are faster to replicate in the network, and may be useful if bandwidth is scarce. Hearn's warning was not a call to modify the protocol or any part of the Bitcoin code at the time, but an advice to miners to keep the network open to the demand of transactions.

Bitcoin's transaction blocks have a limited space to allocate transactions. If a transaction does not make it into a block, it waits in the "memory pool" to be

64 In bullets in the original.

integrated in the next one. By the time of the thread, the memory pool for pending transactions was not clearing them fast enough, because the use of the network was growing. This increase was in great part due to the gambling website Satoshi Dice(‘Bitcoin Dice - Satoshi DICE’ 2017), which allows betting on the information produced by the network. These bets contributed to flood the blocks, thus, the thread advised to ignore transactions involved with Satoshi Dice or to increase the soft limit to deal with them and be able to unblock other non-betting transactions. The controversy of this thread was more focused on what posture to take on Satoshi Dice than on scaling or consensus, however, it shed light on the divergent stances regarding the later block size discussion. Hearn briefly presents the consensus on this matter when user “drawingthesun” complains on the limits of the network: “Bitcoin can't handle more than 1000 transactions a second? There is no way a Bitcoin will have value in 20 years! Why are they so stubborn? This is the single biggest hole in our Bitcoin fantasy.” (*ActionTH*). Hearn’s answer is that developers are not a single unit, and lists some of the most relevant core developers’ postures:

> So, to be clear, ‘the devs’ is not a single unified hive mind :)
>
> I actually want to see the block size limit removed, Bitcoin to scale up, and after that sort of thing is done SatoshiDice type sites won't be as much of an issue anymore. I think Gavin [Andresen] feels the same way, as does sipa [Pieter Wuille]. Not sure how Matt [Corallo] feels.
>
> retep [Peter Todd] doesn't feel that way, however, though he's written some great posts and useful patches, he hasn't been working on Bitcoin as long as Gavin or I have.
>
> Luke-Jr has the most extreme view of all of us, he sees SD [SatoshiDice] as being abusive and filters out their transactions from his pool [Eligius].
>
> I included the option of filtering SD transactions out in my initial post because that's a short-term hack that buys additional time, if for some reason expanding the soft limit is not deemed acceptable or is insufficient. I don't think that'll be the case though (*ActionTH*).

Gavin Andresen, a respected lead developer in the Bitcoin community chosen by Nakamoto (Simonite 2014)[65] reinforced Hearn belief later in the same thread, by stating that in his opinion, "there is rough consensus that the 1MB block size limit WILL be raised. It is just a question of when and how much / how quickly." (*ActionTH*). Andresen seems to think that scaling the blockchain is obvious to most people involved with Bitcoin's future, and that only technicalities, like at which point in time or with what exact method the block size would be raised, are to be resolved. In fact, few people would actually resist scaling, but, as I will show, scaling and block enhancing are not perceived as synonymous. Peter Todd, another developer heavily invested in the project, and gradual rival of Hearn, replied to Andresen that:

> To say there is a rough consensus that the 1MB[66] block limit will be raised at some unspecified time in the future is missing the point. The real issue is, is there a consensus that a large fraction of the transaction volume will in the future happen off-chain? Given the range of opinions between you and Mike [Hearn], who expect transaction fees to stay low enough for all but microtransactions, Pieter Wuille, who if I am correct is unsure, and Jeff Garzik, and Gregory Maxwell, who are both working on designs for off-chain transaction systems, I just don't see a consensus (*ActionTH*).

Finally, Jeff Garzik, another main developer contributing to Bitcoin code since 2010, adds his opinion to the scaling issue: "In general, I would say there is rough consensus that the 1MB size limit *probably* will change *sometime* in the future. But beyond that, opinions vary wildly. I think there is also a rough consensus that unlimited block size is nutters." (*ActionTH*). Like many threads involving a hot topic, it evolves into a diversity of micro-controversies and eventually fades just below the 300th comment. The soft limit was enhanced by default in the 0.9.0 version[67] of the software (March 2014). However, the lack of consensus would become bigger in the future. Another thread, also started by Hearn, and one of the most discussed in the "Development & Technical Discussion" of the Bitcoin forums, proposed a way to fund mining in an unlimited block size scenario, i.e.

65 Andresen was the lead developer of Bitcoin Core from 2011 to 2014. He kept working on the project until the beginning of 2016. In May of that year his Github commit access was revoked by the other core developers, allegedly on the basis that his account had been hacked.

66 One megabyte (1 000 000 bytes of digital information).

67 https://bitcoin.org/en/release/v0.9.0.

assurance contracts. The discussion extended not only because the limitations of the proposed funding technique, but because it set eyes in a scheme that most of the main developers resisted to foresee. Again, Peter Todd plays the main antagonist role, especially on the consensus of block size:

> FWIW [For what it's worth] currently the majority of the core team members, Gregory Maxwell, Jeff Garzik and Pieter Wuille, have all stated they are against increasing the blocksize as the solution to the scalability problem. Each has different opinions and degrees of course on exactly what that position constitutes, but ultimately all of them believe off-chain transactions need to be the primary way to make Bitcoin scale. (...) to be clear no-one, including myself, thinks the blocksize must never change. Rather achieve scalability first through off-chain transactions, and only then do you consider increasing the limit (*InfiniteTH*).

Todd argues against block size scaling because it involves a hard-fork, which, due to its destabilizing nature, requires consensus from most part of the Bitcoin ecosystem. I'll specify later what a hard-fork consensus means specifically, and question the scope of the ecosystem regarding decision making processes. At this point, consensus should be limited to the developers of the core Bitcoin software. Being an open source project, the list of developers hovers around 360, but only a handful of them have permissions to "merge", that is, to integrate proposed changes to the main branch of code. Everyone has a voice (a sound implementation proposal), but only a few have the authorization to enact the voice. New implementations need a reasonable number of AKCs (short for acknowledgements) from all developers participating in the discussion, but a solid ACK consensus of the ones with the power to merge. A general "ACK" means that they agree with the concept and direction of the proposal, but haven't revised the code, a "utACK" reveals that they agree with the idea and the code, but haven't test its actual functionality. A "tested ACK" is a good to go position, both from an instrumental and a philosophical point of view. Finally, a "NACK" position disagrees either with the idea or its implementation, and is usually supplemented with some argumentation. It is not unusual to see participants that disagree with the change, but ACK or utACK depending on the group orientation.[68]

68 At the moment of this writing, eight people were "collaborators", -i.e. have the power to merge- in Bitcoin's Git repository, but neither Peter Todd, Gregory Maxwell, or Mike Hearn, the most intense voices of the block controversy, are or were in this list. The

Being an open source project, the development is in theory open to everyone. This includes not only the coding to maintain the system working and free of errors, which, like in most open source projects is provided by multiple volunteers, but also the ideas to improve the system. Everyone can help in the future design, but all propositions are filtered through a clearly defined policy. The next section explains the procedure for new suggestions, and how proposals were distributed among developers. It also signals the first proposal that called for an expanded block solution for scaling.

BIP 101: Introduction to Code Improvement Proposals

Like most open projects, collaboration issues in Bitcoin can be settled via Git protocols like the ones described above, but due to its delicate consensus requirement Bitcoin development also adds a second layer of conventions for new suggestions. Created by Amir Taaki,[69] Bitcoin Improvement Proposal (BIP) followed the tradition of Internet Engineering Task Force's ('The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force' 2012) open calls for improvement. BIPs are essential for changes are particularly controversial or that introduce changes to core rules of the protocol.

They are organized into three categories: standard, informational and procedural. Standard BIP's introduce changes to the network protocol, block and transaction validation, and in general anything that can affect interoperability. Informational BIP's are concerned with guidelines and design issues. Process BIP's propose changes that take place outside of the network protocol. According to Taaki's protocol, before assigning a BIP number to an idea, it has to be previously discussed in a Bitcoin forum or mailing list. After it has had at least some positive feedback, it can be submitted for a BIP. This process saves time on the person proposing the changes, for if his idea seems particularly difficult to implement or has no support from the community, there is no point in investing time further developing it. BIPs are then, filtered suggestions that earn the possibility to be thoroughly discussed and implement by whoever is interested in participating. The

collaborators were Garzik, Schnelli, van der Laan, Dashjr, Falke, Wuille and Fields; Nakamoto and Malmi are the only people that abandoned it, and Andersen is the only one whose permissions got revoked.

69 He also proposed making donations in bitcoin to wikileaks (Popper 2015, 58).

BIP editor can deny BIP status only when there is “duplication of effort, disregard for formatting rules, being too unfocused or too broad, being technically unsound, not providing proper motivation or addressing backwards compatibility, or not in keeping with the Bitcoin philosophy” (‘Bitcoin/Bips’ 2016). Except for the last one, most reasons for denial are technical and non-controversial, so any technically feasible proposal with enough backup can become a BIP draft. Standard track BIPs include code or a patch to be applied, that is improved while the BIP is still considered a draft. Once this implementation is complete and accepted by the community, the status can change to “final”. If for any reason the BIP stagnates, the status is changed to “deferred”. It can be “rejected” too, when further discussion proves there are unresolvable problems with the proposal (Taaki n.d.).

The block-scaling debate lingered in dribs and drabs through different channels (mainly Reddit and the Bitcoin forums) through 2014 but without a notorious presence outside the internal development discussions. Mainstream media focused more on the steady hand of the coin’s volatility, the follow-up of a myriad of start-ups trying to exploit Bitcoin blockchain, and the curiosity of the banks to adopt Blockchain technology in one form or the other. However, in 2015 a series of (failed) BIPs emerged trying to implement scaling solutions that would more broadly evince the controversy.

The beginning of May 2015 reignited the scaling controversy among developers. On May 4th Andresen posted “Time to roll out the bigger blocks” (Andresen 2015c) and “Why increasing the block size is urgent” (Andresen 2015d) in his personal blog. There he argued for an “ugly but necessary” block scaling (Andresen 2015b). Andresen’s support for scaling was rapidly noticed by the other core developers: only two days later, Matt Corallo started a thread raising concerns about it in the developers mailing list (Corallo 2015). The thread triggered a substantive discussion between the most active collaborators at the moment, but especially between Hearn, Todd, Jeff Garzik, Jorge Timón, and “btc drak”.

Again, Hearn fulfils the role of spokeperson, as Andresen has minimal participation in this mailing list discussion. He and Andresen are the only strong advocates to substantially increase the blocks; the others agree to the necessity of scaling, but not on the forking solution. A day later, Hearn started posting a series of posts supporting block size increase. In these, he pointed out that the time to

implement a decision was getting close, as transactions were near to achieve 100% of the block size, like the soft-fork of 2014. All transactions that don't make it into a block get stored in the memory pool, but as they accumulate, the time to insert them into a block also grows. It is a bloated system, Hearn argues, because at 80% of capacity, half of the transactions would take as long as 20 minutes and, alarmingly, at 100% half of the transactions would take more than 6 hours. A revision of the figures minimized the numbers to a 2-hour delay at 100%('Bitcoin Traffic Bulletin (Redux)' 2016).[70] What followed were a series of diplomatic BIPs by several of the main developers, tackling an implementation for the controversy resolution, and also a seemingly undiplomatic fork lead by Hearn. On June 22, Gavin Andresen proposed BIP 101, an implementation to upscale the size of the blocks to eight megabytes —eight times the current size— in 2016 and then doubling the size every two years until 2036 (Andresen 2015a). This denotes a long scope plan to deal with the scaling issue. Only a day later Jeff Garzik proposed BIP 102, which requested a one-time increase to two megabytes —twice the current size (Garzik 2015). An even longer scope plan was proposed by Peter Wuille about a month later: BIP 103 specifically asked for an increase every 97 days or so, for a constant 18% growth per year, until 2063 (Wuille 2015). "Btc Drak", also a main contributor, added BIP 105 in August, the first of dynamic growth proposals, not subjected to arbitrary scaling, but dependent on the behaviour of the market and/or miners. BIP 105 introduced a function for miners to vote for small increases or decreases every time they created a block (BtcDrak 2015). It deflected all responsibility on block size to miners, and relied on a hypothetical invisible hand (Smith 1791) of production. BIP 106 (Chakraborty 2015) was proposed in the same month and also used dynamic scaling, this time based on the last 2,000 block fillings, i.e. if a majority of those blocks were close to full, the block size doubles, if on the contrary they weren't, the block size is halved. Again, the size is controlled by miners, yet mediated by an algorithm. BIP 107 (Sanchez 2015) was a hybrid version of the previous proposals. It was proposed on August and supported a two MB increase first, then a four MB and six MB between it and 2020, thereafter a dynamic increase very similar to BIP 106. Finally, BIP 109 (Garzik 2016), also proposed by Gavin Andresen in January 2016, after withdrawing his first proposal (101), offered a more modest increase of two MB, but with fine-grained rules, and added precautions to how these changes

70 As a reference, in December 2015, the average capacity was at 60%.

could be adopted by miners: a smaller threshold was chosen to be considered a majority (74% instead of 90%), to avoid the decision to be hijacked by only one of the biggest pools (Andresen 2016).

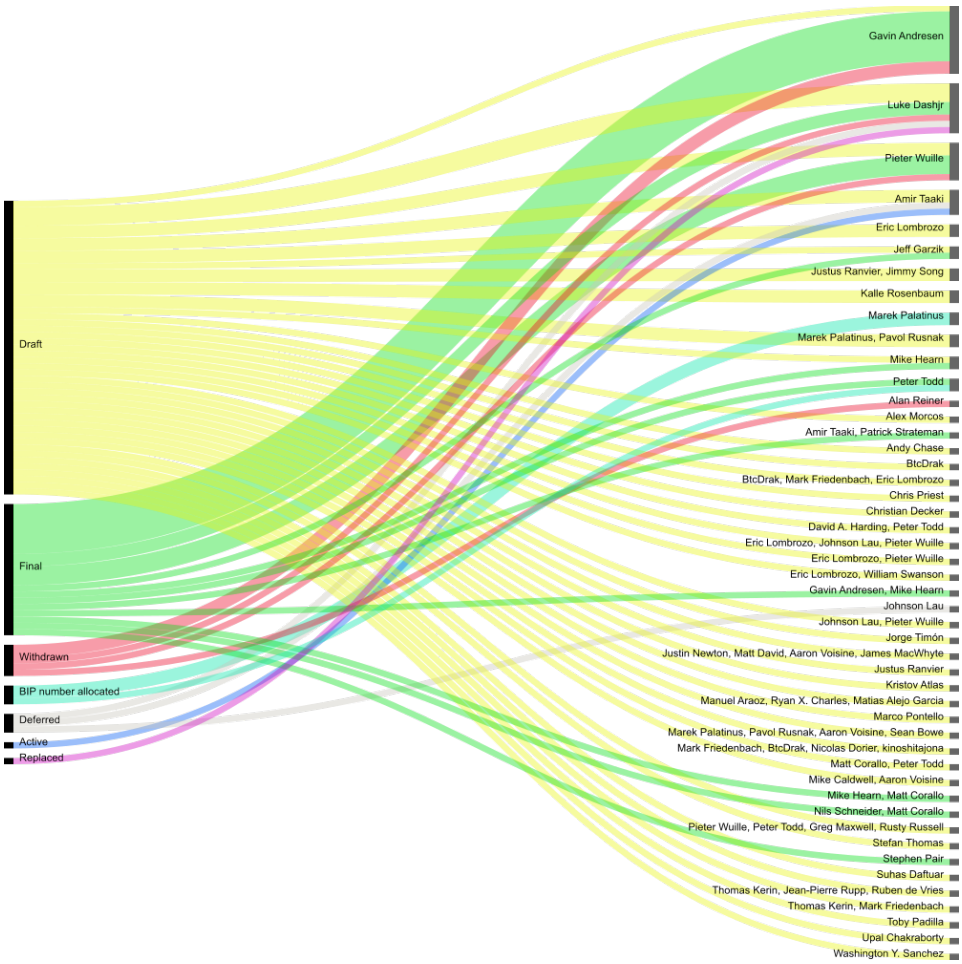

Fig 12: Alluvial distribution of BIPs status and applicant

Except for BIP 101, these BIPs like many others remain on a draft stage, mostly because the ideas in them may be re-purposed for future implementations. For the total 82 BIPs, five have been withdrawn, three deferred, and only one has been replaced. As shown in Fig. 12 ('Bitcoin/Bips' 2016) most of the main developers have proposed changes to the protocol, with different outcomes. It is clear that Andresen holds the bulk of the proposals —eleven, plus one co-authored with Mike Hearn (Andresen and Hearn 2013)— but also that drafts, accepted, and withdrawals are fairly distributed among all developers.

Hearn did not propose a BIP for block scaling. Before, he had already proposed BIP 31, BIP 37 (with Matt Corallo), and BIP 64. The first two were accepted, but the last one generated the usual confrontation with Todd: it was acknowledged and merged, but then reversed, due to a security issue. Instead, Hearn would later implement this BIP and Andresen's 101 in a fork called Bitcoin XT. Forking is a regular activity within open software, and this was far from being the first Bitcoin Fork. However, due to the particular characteristic of being an open software with embedded (and rapidly growing) economical value, a fork outside of the consensus sphere proved to be openly confrontational and generated a break up in two decisive groups.

5.2. Strategies for Dissension: Forking

Forking is a strategy that comes from OSS projects. It is usually limited to open projects because it involved a direct duplication, and thus nothing under subject to copyright can be formally forked (Tkacz 2011). Since the initial state of the fork includes two projects with the same code, followed by changes in each branch, *competition* between them is considered a natural part of forking (Raymond n.d.). As a phenomenon originated from software cultures, forking has been a topic for many scholar works (e.g. Steven Weber's "*The success of open source*"; and Clay Shirky's "*Here comes everybody*"), but it has been mostly discussed within popular "native" contexts. Nathaniel Tkacz argues that there is no single definition of a fork, but it is possible to identify its core characteristics in the literature:

> Forking primarily involves a split, the duplication of source code or content and the creation of a new project along with the original. The two projects proceed in different directions, but, at least initially, both draw on the original code. As the two projects develop in different directions, at some point it becomes impossible to exchange code between the projects (Tkacz 2011, 95–96).
>
> Forking also brings into question the intent of the "forker" and the status of the wider "developer community" who cannot be forked in the technical sense of duplication (Tkacz 2015, 132).

To illustrate his points, Tkacz (2015) critically discusses the 2002 forking of the Spanish chapter of Wikipedia into the *Enciclopedia Libre Universal en Español* ('Enciclopedia Libre Universal En Español' 2017). After internal disagreement regarding the funding strategies for the Wikipedia project, the Spanish version forked its contents and started its own wiki version in Spanish. Tkacz follows the competition between the two projects in relation to number of contributors and published articles, up until 2011. While at the beginning both are in direct competition, by the end of this period the Spanish Wikipedia (the original branch) had a significant advantage (e.g. 15,706 active users compared to 67 in the Enciclopedia Libre fork).[71] Tkacz analyses the capacity to fork in the context of Hirschman's "exit" and "voice", as options for dissidence. The first by abandonment and the second as an attempt to change practices of an organization (Hirschman 1970). Forking, then, can be read as a way to "respond to the question of (perceived) organizational failure, deterioration, or discontent in different ways" (Tkacz 2015, 129). Edgar Enyedy, the leader of the Spanish chapter of Wikipedia, used forking as a way to both voice his concerns on the "free" status of the project, which to this date relies on voluntary donations, and to exit when internal negotiations reached a dead end.

In the case of the block size controversy, Hearn can be identified as the "forker" figure, since he was the one that trespassed the BIP proposals to implement a hard fork. The clustering of antagonists is more complicated, considering that most BIPs included their own kind of block scaling, however, it is clear that most of the "developer community" supported following the consensus path and to keep looking for options to scaling before any implementations. Andresen is the exception: he was keen to support every direction possible: he discussed new BIPs, offered their own, and helped coding Bitcoin XT (whose first version was practically based on his BIP 101) all at the same time. For Andresen, known within the community as a respected voice, scaling was the problem and any working solution for it was the correct answer to that problem:

71 Tkacz considers that end of competition is not synonymous with a political failure of the fork: "The fork demonstrated that the issues at stake were serious enough for contributors to leave, and it elevated the force of the debate that transpired on the list, along with its repercussions" (Tkacz 2011).

> I AM considering contributing some version of the bigger blocksize-limit hard-fork patch to the Bitcoin-Xt fork (...) and then encouraging merchants and exchanges and web wallets and individuals who think it strikes a reasonable balance to run it. And then, assuming it became a super-majority of nodes on the network, encourage miners to roll out a soft-fork to start producing bigger blocks and eventually trigger the hard fork. Because ultimately consensus comes down to what software people choose to run (*ReigniteTH*).

Tkacz identifies two main qualities to forking: its "constitutive" nature and its function as a "safety net" (Tkacz 2015, 133). The first one is seen as the basic right or freedom (S. Weber 2004) to fork, embedded in open software projects. Indeed, Bitcoin as an open source project offers that constitutive right, and the core software has been forked more than a thousand times: most of these forks exist as a practical way to commit changes before submitting them for integration into the main repository, it is fair to assume that many others are orphaned experiments (the git protocol and the Github website allow to fork a repository with a simple command line or by pushing one button).

Similar projects to Bitcoin were generated and ramified from this original source code to produce competing coins. Dubbed as "altcoins" or "bitcoin-derived cryptocurrencies"('Build-a-Coin Cryptocurrency Creator' 2017), most of them emerged as competing cryptocurrencies that behave differently. *Litecoin*, the second largest cryptocurrency to date, is an example of a competing coin. It behaves as a currency, but uses a different hashing algorithm (scrypt, instead of SHA-256) with the intention of complicating the use of ASICs (see Chapter One) in the mining process. It also modifies some of the Bitcoin variables, like having a faster block processing and a maximum of 84 million tokens. Litecoin has its own code branch, name and blockchain, which distinguish it from the Bitcoin chain. It does share, however, the financial asset orientation. Thus, it can be considered a competitor within the cryptocurrencies market but, it remains an independent chain and coexist with Bitcoin and other altcoins.

A few other projects do not even enter in direct competition with Bitcoin, because they use tokens merely as mediums for other ends (e.g. distributed DNS servers). Like the competing coins, these blockchain instantiations keep basic characteristics of any blockchain —a shared registry that conflated its own token circulation and production— but are not identified as currencies or economic

elements. Thus, they are neither competing chains nor competing coins. *Ethereum*('Ethereum Project' 2017) is perhaps the most known example. At times coined Bitcoin 2.0, Ethereum is not seen as an altcoin or as Bitcoin evolution, but as an artefact that enhances the original scope of mere circulation by introducing a programmable and executable aspect to the blockchain. Commonly known as digital contracts, these are arrangements and rules defined between two or more parties and deployed in Ethereum's blockchain. While "ether" function as tokens to enable the contracts, they are seen more as "activation" tokens than as crypto-money. Ether does have a monetary value, and like Bitcoin is bought and sold in relation to fiat markets, however, the economical exchange plays the role of a mean to the end of generating and executing digital contracts.

However, unlike Litecoin or Ethereum, Bitcoin XT was presented as direct competitor for the same *chain*. Competing chains are attempts to replicate the same blockchain in order to replace it. While changes are regularly made to the code and protocol of the Bitcoin blockchain, the intention to upscale the size limit in the blocks of transactions, generated the intention to create competing bitcoin blockchains to the original chain (simply called "Bitcoin" or "Bitcoin Core"). Curiously, Bitcoin XT would not even be the first fork using the same blockchain and mint: Bitcoin LJR (Dashjr n.d.) has been maintained by Luke Dashjr, a main developer, since 2011. Bitcoin LJR introduces minor changes, and should in theory be considered a direct competitor of Bitcoin Core. In reality, however, it has played more the role of a reliable experimental backup and its "false competition" is of another kind than the controversial Bitcoin XT. Like Dashjr, Hearn had always the constitutive freedom to fork and start his own project as he is abruptly reminded by Todd in a heated BIP discussion:

> Of course, the beautiful thing is that we don't need consensus: you can always create a Bitcoin Core fork for people who want to volunteer to provide decentralized and unauthenticatable services to others if you can't get consensus that doing so is a good idea. (...) It'd also make it easier to implement things like proof-of-passport to (perhaps) give some assurance that your peers for these services aren't sybil attacking you - all things that can easily be done in a fork you're leading the development of (*Bip64TH*).

The purposed changes of the BIP 64 would in fact be eventually added to Bitcoin XT code, for which creation Hearn appealed to "safety net" function. Forking as

“the last resort of the disgruntled” (Tkacz 2015) when all communication channels haven been closed. In an interview with The Guardian Hearn stated: “I feel sad that it’s come to this, but there is no other way. The Bitcoin Core project has drifted so far from the principles myself and many others feel are important, that a fork is the only way to fix things” (Hern 2015). The idea that the Bitcoin XT fork was the only solution to the whole scaling problem is in great part the reason why this particular fork generated so much controversy and rejection.

Like the LJR fork, Bitcoin XT competes for the control of the same blockchain, but unlike LJR it aroused the community, for two reasons: First, it blossomed in the middle of an existing controversy, which had been silently growing for some years and appealed to the “right” principles of the project. And second, it was a direct confrontation of the whole idea of consensus. I’ll come back to the idea of the “right” Blockchain later, and focus now on the confrontation generated by XT. In the context of an increasing mood for changes in the state of affairs of the Bitcoin ecosystem, and a strict law to implement them based on consensus, Hearn’s fork was clearly a contentious dissidence. Even that both consensus and fork are an integral part of open software, the fork must be read here as the antithesis of consensus. Bitcoin’s distention is enabled by the move of different forces, atomically represented in the BIP’s implementations and the collaboration to expand the code based on the necessities of the ecosystem (conformed by quite diverse entities: from irregular contributors to the code, to CEOs of start-ups involved with the cryptocurrency, or lawyers dealing with regulation issues). The necessity to scale, regardless of the block size disruption, is intentionally executed by Hearn’s fork. This intention to distend triggered the already existing opposing forces of the Bitcoin project to the point of break up. Thus, it is important to discern that the “forker”, —Hearn, and Andresen to a lesser extent— and the opposing “dev community” are but the placeholders of a sum of vectors. With this in mind, it can be observed that the fork clustered two groups.

De-Sideing the Blockchain

From an uninformed perspective and because the debate concentrates around the word "scaling", it may appear that the groups are divided by their intentionality, or lack of, to scale. Indeed, Hearn constantly accused his antagonists to intentionally block Bitcoin's growth: "those who don't want to see Bitcoin scale up as Satoshi intended have decided to stall the process of doing so" (Hearn 2015). He directly accused Peter Todd of not wanting Bitcoin to scale up (*InfiniteTH*), and argued that the Chinese miners also had infrastructural reasons to oppose to scaling by any means:

> Why has the capacity limit not been raised? Because the block chain is controlled by Chinese miners (...) Why are they not allowing it to grow? (...) the miners refuse to switch to any competing product (...) and they're terrified of doing anything that might make the news as a "split" and cause investor panic (...) And the final reason is that the Chinese internet is so broken by their government's firewall that moving data across the border barely works at all (...) This gives them a perverse financial incentive to actually try and stop Bitcoin becoming popular (Hearn 2016).

On a previous post, however, he had included "several major mining pools, including all the Chinese pools" (Hearn 2015) in the list of entities supporting raising the block size. The purpose of this post was to justify the creation of Bitcoin XT (both posts were published in the same day). The list did not directly name anyone but Gavin Andresen and Jeff Garzik, and included: developers of popular wallets, many bitcoin exchanges, the two biggest payment processors (presumably Bitpay was one of them), and users in online forums. The list was partly based in a previous compilation by Reddit user "Technom4ge"('List of Bitcoin Services That Support/Oppose Increasing Max Block Size' 2016), who gathered statements of notorious names in the Bitcoin industry. It must be stressed that these clusters were malleable, and many supported a hard-fork, but with different specificities and not necessarily the specific version proposed in Bitcoin XT. The latter was, nonetheless, the only existent implementation at the moment.

Here it is important to discern between scaling and hard-forking. Far from Hearn's claims, no one in the Bitcoin ecosystem publicly supported stagnation, as it was in everyone's best interest to extend Bitcoin's use and capabilities. The real issue was to what point to scale, and by what means, and this is where the ecosystem was divided. The cluster represented by most main developers was in favour of scaling not by enhancing block capacity by hard-forking, but by scaling

through any other feasible means. On the other side, the group represented by Hearn, had no problems in changing block size (this last option was, from a technical point of view, as easy as changing a line of code).

At some point during the forum's threads, Hearn stopped addressing each member personally and started clustering on *Blockstream* what he identified as an opposing force. Blockstream is a Blockchain technology company co-founded by Gregory Maxwell, Mark Friedenbach, and Adam Back. Maxwell is one of the main developers, and like Peter Todd, a constant antagonist of Hearn. Blockstream develops sidechains (Back et al. 2014) and the *Lightning Network* (among other projects), both intended to ease the transaction load on the core blockchain, and enable communication between it and other blockchains, while monetizing the process. The president, Adam Back, is a long-standing figure in the cryptography community (author of Hashcash, as seen in Chapter Three). He had suggested in August 2015 an immediate block scaling of two MB, followed by a four MB in two years, and eight MB in eight years (Back 2015), but he also stressed the importance of developing other forms of scaling, like the ones Blockstream would eventually develop. The company raised 21 million in investments in November 2015 (Rizzo 2014) and 55 more in early 2016 (Vigna 2016). In the reignited discussions of 2015, Hearn addressed the resources of the company and clustered his criticism in the organization rather than in specific developers:

> the 'Bitcoin ecosystem' is not well funded. Blockstream might be, but significant numbers of users are running programs developed by tiny startups, or volunteers who don't have millions in venture capital to play with. (...) What I would like to see from Blockstream is a counter-proposal (R*eIgniteTH*).

Blockstream's payroll certainly includes Maxwell, Jorge Timón, Mark Friedenbach and Pieter Wuille, all Bitcoin Core maintainers. The company then would remain a strong "side" of the controversy even after the failure of Bitcoin XT and Hearn's disappearance. The successor of XT would be another failed fork, Bitcoin Classic, also supported by Gavin Andresen and other parts of the industry, which expressively stands against Blockstream's influence over Core development.

Decentralization of Unforkable Money

The strongest arguments in favour of size increase (in any of its forms) can be summarized as the easier and more straightforward method for scaling. The reasons to refuse it are less unequivocal. When BitcoinXT's adoption was being discussed, Gavin Andresen gathered a list of the main arguments against block size scaling (Andresen 2015c). Many of them are related to security, stability, efficiency, and existence of implementations, yet one of them stands out from the rest, and is summarized as: "More transactions means more bandwidth and CPU and storage cost, and more cost means increased centralization because fewer people will be able to afford that cost." (Andresen 2015e). The decentralization issue is particularly relevant within Blockchain technology, but crucial to the Bitcoin project, as it is by definition the first decentralized network of its kind.

Peter Todd's repeated concern with the scaling issue is not only related to instrumentation ambiguities, but with centralization and (state or corporation) censorship. Unlike other main developers like Andresen, Wuille or van der Laan, who tend to avoid confrontation and focus on settling technical disagreements, Peter Todd would play the role of direct confrontation with Hearn, by focusing on the ethics and ends of blockchained systems. As early as February 2013 (*InevitableTH*), Todd argued that a fluctuating or unlimited block size would "inevitably" lead to a centralized system. While his thread used far-flung examples for the actual fork proposals —blocks of ten megabytes, 100 megabytes and even one gigabyte in size— is still valid: a miner with better bandwidth has a better chance to distribute a block trough the network (it can send the same amount of information to more people), and therefore win the race for integrating his block on the chain. A hypothetical competing miner, dubbed "David" in Peter Todd's argumentation, who "lives in country with a failing currency, and his local government is trying to ban Bitcoin" (*InevitablyTH*), has a strong disadvantage and can't effectively win the race to find new blocks, thus, abandoning mining or joining a pool. The pools, however, would eventually be in the same dilemma, and only the ones with infrastructural advantages would remain, geographically clustered. This is, effectively, the centralization anxiety of the distributed system, brought by bigger blocks in the chain.

Infrastructure deficiencies were a restless element for miners in China since before BIP 101. When Gavin Andresen informally proposed an increase to 20 MB blocks, five of the strongest Chinese mining pools pronounced against it, and

in turn made a compromise for an eight MB increase, arguing that “Chinese internet bandwidth infrastructure is not built out to the same level as that of other countries” and that “Chinese outbound internet bandwidth is restricted, which causes increased latency in connections to Europe and the United States” (van Wirdum 2015). The signers, Antpool, F2Pool, BTCChina, BW mining, and Huobi, gathered at the time more than 50% of the hashing power of the whole network.

Hearn, in contrast, is not interested in *David’s* (or the chinese miners) luck: “You want to keep the block size limit so Dave can mine off a GPRS connection forever? Why should I care about Dave? The other miners will make larger blocks than he can handle and he'll have to stop mining and switch to an SPV client. Sucks to be him.” (*InevitableTH*). Even though Todd does not claim to defend vulnerable miners, he makes it clear that decentralization and security are his and Bitcoin’s main ends: “I don't have any interest in working on a system that boils down to a complicated and expensive replacement for PayPal. Decentralization is the fundamental thing that makes Bitcoin special.” (*InevitableTH*). The discussion generated more than 500 comments, extended for almost two months, and aroused the debate.

What is at stake here is that scaling the network has a decentralization cost, which in theory goes against the fundamentals of Bitcoin. The cost may be acceptable, since every entity is up for enlarging the system, if the outcome is worth it. In this case, the goal is what divides both groups. Jeff Garzik questions this very issue in the middle of 2015: "Are we trying to build a system that can handle Paypal volumes? VISA volumes? It's not a snarky or sarcastic question: Are we building a system to handle all the world's coffees? Is bitcoin's main chain and network - Layer 1 - going to receive direct connections from 500m mobile phones, broadcasting transactions?" (*ReigniteTH*). At stake was not only the capacity of the network to be a system handling VISA payment volumes, but the motivation to create such a system. The Bitcoin XT group argues that the system should be a competitive payment network capable of micro-transactions. The other group argues for a pure core that acts as a ‘settlement network’ (Hagelstrom 2016), which depends on separated, and more centralized, payment networks (i.e. sidechains or the Lightning Network). The purity of the core was one of the reasons why Hearn’s BIP 64 was in fact controversial: while it didn’t pledge to make changes to the block size, it was qualified as an unnecessary change to core,

which “should stay pure and focused” (‘genjix’ *Bip64TH*), and Hearn’s implementations should be written on more superficial layers of the bitcoin code. As I stated before, one of the reasons why this particular fork became controversial was that it questioned the “right” principles of the project, which ended up signalling to different directions.

The breakup of an internal logic within the project is an expected outcome for the fork. As Tkacz argues, a fork is the symptom that the controversy has reached a limit for internally driven negotiation: “When the possibility of a fork emerges, the controversy cannot be settled within the current rules of formation” (Tkacz 2015, 173). This destabilizing effect makes two similar (but not identical) projects go into competition, but the result of this opposition also has a stabilizing effect, because it enables a definite form (the winner) of the open project (Tkacz 2015, chap. 5).

While the stabilizing effect should apply to Bitcoin forking, and in theory to every open project based in Blockchain technology, its money-like behaviour insulates Bitcoin from other Open Source projects. Unlike the Spanish Wikipedia (Tkacz 2015), or the Openoffice.org/Libreoffice fork, where the assets can be replicated and hold their value, the tokens of Bitcoin only have value in one of the blockchains. Open code can be duplicated, but there is only one blockchain, or at least, one that preserves a substantial economic value. It is possible to download and use Openoffice.org or Libreoffice, although the fork took place in 2010, and the main difference are the communities supporting it: on the one hand a corporation and on the other a foundation. Although the Enciclopedia Libre en Español cannot be considered to be in direct competition with Wikipedia anymore (Tkacz 2015, 147 note 16), it is still active and usable for its intended purposes. Coexistence after competition does not apply to Bitcoin, and therefore the fork controversy is different from other open source projects. The reason for this is that the essence of blockchain technology is to oppose digital counterfeit, specifically to avoid double spending on transactions without the need of trusted parties. Even though it is prone to errors, like any other system, the formal materiality (Kirschenbaum 2007) of its pieces differs from other “immaterial illusions”: the “identification without ambiguity” (Kirschenbaum 2007, 11) is deliberately taken to a limit. Unforgeable but fluid pieces of data (or strings of symbols) is the raison d’être and distinctive ontology of blockchains. In the case of Bitcoin, these tokens

are now embedded with economic value. The assets contained in it, not in the software per se but in the network running it, are now worth seven billion dollars, and it is reasonable to expect this figure to grow. The value cannot be split between the forks, assets that remain in the defeated blockchain become worthless. Thus, the outcome of the fork represents not only the future of the project, an ideology for or against centralization, the endurance of a group of people, or the restructuration of consensus rules, but also a substantial economic interest.

Due to these reasons, the struggle generated notorious resistance, and Bitcoin XT never reached the status of an official fork. Despite having the support of part of the industry and an unmeasurable portion of the greater community of users and enthusiast, it lacked the backing from the biggest miners. At its highest point, support for Bitcoin XT was expressed by 10% of the nodes in the network, far from the 75% required for its adoption ('Scalability Debate Continues As Bitcoin XT Proposal Stalls' 2016). Instead, the main developers activated a technique (*Segregated Witness*) to free space from each block by getting rid of non-essential information. Thus, the block size remains to this date at one MB, but each block can manage more information about the transactions. However, the group in favour of the block-scaling did see an implementation: in August 2017, *Bitcoin Cash*, the first chain competing fork was launched('Bitcoin Cash' 2017). Inspired by previous block-scaling proposals like Bitcoin XT, Bitcoin Cash implements an immediate block size of eight MB. As of August, users are able to decide on which chain they want to bind their assets. It is reasonable to expect a non-traditional, in terms of old-school forked open software, competition between these projects in the following months.

The clash not only divided the project into two groups representing "largely incompatible"('Bitcoin Cash' 2017 F.A.Q) visions for Bitcoin. It also signalled the evolution of a contradiction nested in the utopic origins of the project for crypto-assets. This contradiction was noticed in the previous chapter: on the one hand, the project was born from an accumulated concern for privacy —in particular against state surveillance— and decentralization of trust and normativity (as presented in Chapter Three). On the other hand, the project is also the result of a

quest for a frictionless exchange system, able to operate independently from the state structures. Both ends are met and embodied in projects like Bitcoin, however, it is exactly a discussion between which of these ends has ultimately a higher priority, what branched a somewhat cohesive ideology into two separate programmes represented by Bitcoin Core and Bitcoin Cash. Competition between the two projects is also convoluted, in comparison to other OSS examples, by the particular characteristics of the public blockchain of being at the same time an open and public digital machine, yet producing private non-duplicable units. The birth of the blockchain is a cause for reformulation of the notion of forking in OSS, and the attempt to fork an effect of the historical contradiction of the machine.

Interestingly, the competition within the system also showed the limitations of the governance that the blockchain system itself is, in part, trying to avoid. Coming back to Gregory Maxwell words at the beginning of this chapter, "mankind is ill-equip to create a strong and sound system via human governance (...) mankind is fundamentally not cut out for it (...) Bitcoin was specifically created and promoted to replace that kind of subjectivity with machine". In a way, this chapter closes a circle with the first one. It connects the humanly settled production of an idea —*the* Bitcoin blockchain— embodied in a machine ruled by the efficient logic of automated computation, whose utmost purpose is to replace or outsource a process of production and (tentatively) of governance. This circularity is performative and touches the social and the technical without establishing a decisive causality in between them. The blockchain system performs in a deterministic manner, it is a working expression of a process of production almost entirely outsourced to the computational; yet, as I partially have showed in this chapter, it is itself performed in a non-deterministic way, and its evolution is marked by the political struggles and limitations of governance.

Abbreviated references

ActionTH: Soft block size limit reached, action required by YOU. (2013). Retrieved 7 September 2017, from https://bitcointalk.org/index.php?topic=149668.0;all

Bip64TH: Add a getutxos command to the p2p protocol. (2014), Retrieved 7 September 2017, from https://github.com/bitcoin/bitcoin/pull/4351#

InevitablyTH: How a floating blocksize limit inevitably leads towards centralization. (n.d.). Retrieved 7 September 2017, from https://bitcointalk.org/index.php?topic=144895.0;all

InfiniteTH: Funding of network security with infinite block sizes. (2013). Retrieved 7 September 2017, from https://bitcointalk.org/index.php?topic=157141.0;all

MinnersupportTH: Wondering out loud: Which should Chinese miners support - Core, Classic or another? (2016). Retrieved 9 September 2017, from https://bitcointalk.org/index.php?topic=1343716.0;all

ReigniteTH: Hearn, M. (2015). [Bitcoin-development] Block Size Increase. Retrieved from https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-May/007885.html

Conclusion

This thesis provided a critical overview of blockchain technology by reflecting on the historical, geographical, and organizational characteristics of Bitcoin. Each approach paid attention to the reconfiguration of power dynamics occurring in relation to the performance of this technology. The work offered a close study of the technical structure of Bitcoin, and discussed it in relation to notions of authority and legitimacy. The study showed that blockchain technology participates and enhances a computational redefinition of the former notions. This was demonstrated by highlighting the importance of the technical arrangements participating in the general performance of Bitcoin, and by contrasting them with the shifting relevance of canonical governmental institutions.

I showed that Bitcoin is a relevant example of how administrative duties related to the modern state are outsourced to state-independent computational systems. What is more, in the case of Bitcoin, notions such as authority and legitimation are not replaced by a defined non-state institution, such as a technology corporation. Instead, I argued that authority and legitimation are integrated into the technical system. This shift brings with it not only the use of technological tools for the composition of more efficient administration services, but also the generation of new political, spatial, and organizational arrangements modelled on the computational ontologies and epistemology of these digital devices. Each chapter paid special attention to the former dimensions by developing four notions performed by the blockchain technology of Bitcoin — authority, prehistory, space, and governance. I argued that these subjects are intertwined by four different understandings of “utopia” that evince internal contradictions between the rhetoric associated with the blockchain and with its operation.

The first chapter provided a political theory framework and a discussion on the process of mining to illustrate how authority is performed in the blockchain’s system of production. In it, I showed that Bitcoin is a system that has a particular absence of authority figures. I expanded this argument by claiming that while a few different entities tried to legitimize their positions, none of them

is able to fully claim the system's management. I then argued that a novel notion of authority is displaced towards the technical processes that manage the production, and that these processes are coded within the systems efficiency and technical performance. I presented a detailed description of how mining works, as this process represents a folding of the groundbreaking technical operation of blockchains. Mining is in my reading an expression of a superabundance model present in digital forms and exploited by Bitcoin: the model uses randomness and intensive calculation to provide stable efficiency. The latter is prioritized above consumption of resources and waste, and becomes the basis on which to provide an institution-independent notion of *countability* based on automated production and exchange.

I claimed that the lack of a clear external authority and the instrumentation of management through efficient computation are core elements to understand the power rearrangements brought about by this kind of technical system. Finally, I identified that the specific technical configuration of the production process, which closely combines a public network with private tokens, sheds light on the multiplicity of projects gathered around the promise of the blockchain. This particular configuration of production inspires different entities with dissimilar goals. Production in Bitcoin, then, not only outsources political expressions of power such as authority and legitimation to the machine, but also feeds disparate political projects due to its combination of public and private elements.

The second chapter clarified core notions used throughout the thesis, and questioned some issues of my own methodology. I also offered an argumentation for reading cryptocurrencies as a medium, not only due to their circulating properties, but also by taking into account previous academic literature relevant to my theoretical framework and the goals of my analysis. On this chapter I narrowed my distinct use of the term "political" in relation to STS literature, and questioned the problems of thinking about digital objects by depending on digital techniques to observe them. I stressed the recursive nature of digitally-oriented research, and the importance of recognizing the changes that come with such recursivity: not only regarding the instrumental role of the technical tools used to query technical objects, but also the ontological and epistemological transcoding that takes place with such research practices. I limited my thoughts on this topic to a self-

reflection, and a call for an awareness of recursivity. However, this is a long contested issue and much more can be said of it than is examined in this work.

Chapter three traced different trajectories to make sense of the emergence of Bitcoin, both as a technical system and as a political ideal. By making use of Hu's notion of prehistory —which explores the infrastructural and metaphorical expansion of media— and an observation of Bitcoin as a confluence of different technologies, I presented three different lineages that thread the emergence of the technical object, and the multiplication of its uses. These trajectories were informed by a foucauldian reading on the material relation of power and technology, as well as by Media Theory concerns on how power dynamics can be decoded from digital media. The trajectories divide three moments of concern tied to the development of technical components (gears), discourses, and project deployments of which blockchain technology is made: secure communications, political manifestos, and creation of crypto-money.

The first trajectory of secure communications expresses concern to develop security communication tools. This trajectory is much more involved with large-scale geopolitics and military jurisdiction. I stressed the notion of code as command, as in this trajectory the use of cryptographically techniques is strongly related to national security and exclusively managed by institutional hierarchies within the state. The increasing availability of computation and a growing concern with the US government's uses and management of cryptographic tools paved the way for a lineage that manifested with the democratization of cryptographic technology. I identified this second trajectory with strong political positions appended to media and communications technologies. This trajectory read code not only as a tool, but also as political praxis. The notion of code as command widened to be thought of also as a normative characteristic. The antagonistic position of this lineage saw in code an opportunity to replace an established order and to provide code with a political performativity. This positioning informed plenty of the imaginaries associated with the internet of the 90s, but also prompted the pursuit of replacing state functions with mathematically automated procedures. A specific replacement of this kind was sought by the third trajectory: the attempts to create a digital version of money that was not entirely legitimized by state authority. This lineage was characterized with the explicit intention to produce natively digital financial assets (a digital version of cash). I presented

some examples of these attempts and their shortcomings to generate a functional payment system, that is, not only technically capable of performing exchange tasks, but to do it in accordance to the political ideals of secure and free-of third parties communications. Bitcoin was the system that appeared to comply with the previous requirements, which was a significant reason for its success in the cryptographic and libertarian communities. I argued that the materialization of the third trajectory in the Bitcoin system extended the techno-political performativity of code, from its command and legitimation associations, to the level of production.

This chapter contained a second notion of utopia: an imaginary of ideal conditions expressed through the intention to build a frictionless exchange system imbued by the political. I claimed that the landscape brought by this utopian impulse is also partially responsible for instilling blockchains with a celebratory rhetoric on technology. I suggest that blockchains are popularly marked as a utopian machine, especially in relation to the figure of the state, due to the crossing of the suggested lineages in the formation of Bitcoin. However, this utopian element contained also an early sign of a future crucial struggle in the development of the Bitcoin project. As shown later in chapter five, the needs for privacy and decentralization are not synonymous with the demands for a free market space and competition, even though these elements were combined by the previous trajectories.

If chapter three sought to shed light on the history of Bitcoin in time, chapter four expanded the awareness of the Bitcoin phenomena by providing a discussion of its spatial arrangements. Through the use of digital methods, this chapter traced an empirical map of the Bitcoin network for a specific period. It discussed the relevance of the geopolitical history of the internet to understand the non-territorial space sought (again) by blockchain distributions. Like the rest of the thesis, this chapter highlighted the relation between the figure of the state, in this case in relation to the notion of territory as technology of power. Blockchains inherit part of the cyberspace idealism on the possibility of using technological infrastructures to construct new forms of power distribution. The literal notion of utopia as a both goal and no-place illustrates this desire. I challenged the assertions that perceive a real distribution brought by blockchain networks. My research on the geographies of the actual Bitcoin network performance showed

that this technology is affected by territorial borders and geographical distribution, and is locatable to some degree.

Mapping the network via digital methods allowed me to trace the limits and limitations of the Bitcoin discourse on spatiality: the analysis of the gathered data facilitated some understanding of the migration of certain actors, and the relevance of state-nations in the movements of the Bitcoin ecosystem. On the other hand, the blank spaces left from the use of this methodology also made evident the limitations of trying to thoroughly grasp the blockchain phenomena from a geographical point of view. Finally, this chapter argued that these kinds of networks are able to perform independent of such geographies. I found that these networks are a middle point between the influence of nation-states and independent non-territorial dispersion (stacks). I made use of the concepts of standardization zones and imbrications between state and non-state entities to provide an image of the kind of links that are at play between territorial and non-territorial distributions.

The final chapter observed issues generated within Bitcoin's development. It played the role of a case study of the internal governance Bitcoin's development, and sought another way to approach the question of "how" power relations are performed in Bitcoin by offering a close look on the empirical governance of the system. The close observation of decision-making processes in the current configuration of Bitcoin allowed me to identify opposing vectors of action and their respective rationales. This section was concerned with building a 'map of agencies' by closely observing one of the biggest controversies in Bitcoin's evolution —the block scaling controversy— through the analysis of discussions and decision-making guidelines of the main developers. I identified that its monetary ontology clashed with basic open source software guidelines, thus complicating conventions of conflict resolution within open development. I argued that its monetary properties especially challenge the traditional and key open source characteristic of forking.

This chapter indicated that the struggle between privacy and competition mentioned in chapter Three played a significant role in the separation of a previously cohesive community. The discussion of the controversy's evolution made clear that the outcomes expected from the system were not the same for everyone. This branching depicted not only the intention to fulfil different projects

through the same technological means, and even departing from an apparent shared system of beliefs, but in a way it also revealed the failure of attempts to govern through protocols of technology. The fourth notion of utopia is the particular expectation to replace the continually failed human interaction to produce agreements, trust, contracts, and compliance between parties through technological means. The chapter depicted the close and circular relation between the production of computational determinative systems —aimed to improve human governance— and the non-deterministic organizational processes that produce these systems.

This last chapter acts as a leveraging study against the deterministic readings inherited from the historical ideologies narrated in the third chapter, and the outsourcing of production argued in Chapter One. While I do raise a question on the actual outsourcing of an enacted notion of authority, from traditional political institutions to computing schemes, it is important to stress that this production is surrounded by the social and political subjectivities of its design. The evolution of the digital object does not happen in isolation: affective and social controversies steer the machine that reformulates authority in the production. The analytical considerations that built Chapter One should be considered under the light of the social arrangements happening in the fourth chapter. The unresolved antagonism between the first and fifth chapter can be read as the impossibility of depriving politics of the social, even with state-of-the-art technological arrangements. In this sense, the equilibrium of the protocol is better tuned with the notion of provisional hegemonies (Mouffe 2000) once the elements of governance involved in their design and evolution are considered. No representation of the blockchain (outside of a narrow discourse) exists as an isolated agency, but as an entangled gathering. The unique innovation of blockchain technology effectively delegates authority, sovereignty, and trust unto its system in the form of mining, thus redistributing these notions from normative and institutional entities towards computational schemes. The design and distribution of this digital object is, however, immersed into sociopolitical spaces a shown in Chapter Five.

This thesis offered a critical observation of the blockchain phenomena and how its performance rearranges power structures. It contributed to develop a political theory that considers novel digital elements and is informed by their infrastructures. This work observed the Bitcoin blockchain from a diversity of perspectives to provide a comprehensive understanding of this phenomenon: regarding its operation, the discourses generated around it, and the bridge between the two. While I have provided a cohesive map of the power dynamics in the blockchain, I would like to think that this work helps not only to provide relevant and original knowledge on the subject, but that it also opens up a new array of inquiries for further discussion. In particular, the new (and multiple) generation of blockchain-related projects expand the uses and discourses of this technology, and thus enlarge a field of ontological and epistemological configurations to be addressed.

Glossary

Bitcoin

Bitcoin is a digital software/protocol that combines cryptographic techniques with peer-to-peer technology to enable secure exchange of information without the necessity of a centralized authority. It was originally authored as protocol in November 2008 and implemented as software in January 2009, by Satoshi Nakamoto (a pseudonym representing an unknown individual or group). Being an open project, many developers have contributed to the evolution of the protocol rules and software code since then. Bitcoin was envisioned as a direct payment system and has worked mainly as such. However, the basic concept of a distributed cryptographic database (generally known as Blockchain or Distributed Ledger Technology) has been replicated in a multiplicity of projects. As of 2017, Bitcoin remains the most used cryptocurrency, with a circulation of over 16 million bitcoins (tokens of account within the Bitcoin system).

Block

A block is bundle of information of transactions made in a blockchain. A blockchain is designed so that each new block retains identifying information (hash) of the previous block, thus chaining (or stacking) groups of transaction in such a way that modifying information on a block requires to rebuild all those that follow. The operation to build new blocks (mining) is computationally demanding (it requires intensive processing power), thus, the rebuilding of a chain is close to an impossibility in the system. Each block contains, in addition to the previous block information, a timestamp, a nonce (a random number), and a list of transactions. This information is cryptographically hashed, to generate a hexadecimal string, i.e. the block.

Block-scaling

A significant issue of Bitcoin's design is its compliance for scaling. Its configuration up until 2016 was arranged to manage an average of 7 transactions per second (commercial payment systems like Paypal or Visa can handle as much as 100 and

4000, respectively). As the demand and use of Bitcoin grew, a call to expand this limitation was progressively raised. The technical design of Bitcoin allows to modify the data size of every block generated (currently a hard limit is set to 1 megabyte), a solution that potentially allows the system to scale without major technical restrictions. However, this fix arguably jepardizes its high degree of decentralization. Thus, the scaling through-blocks-size option generated one of the major internal controversies within the Bitcoin community (discussed in depth in the fifth chapter of this thesis). As of 2017, other solutions to scale the number of transactions without compromising the block size original limit have been proposed and implemented in Bitcoins original blockchain, while branched chains have opted for altering the block size.

Blockchain

The blockchain is a distributed ledger of transactions in the form of stacked (or chained) blocks. Each block contains information of the previous one, thus working as a concatenated database. The database is not centrally stored, but replicated in all computer nodes belonging to the blockchain network (this can be private network, or, in the case of the Bitcoin protocol, open to everyone). Each new block generated by the process of mining is broadcasted to every node on the network and appended to the chain. If two different blocks are generated at the same time, the one with the strongest distribution becomes part of the chain. This means that a single chain has “orphan” ramifications. The highly praised security of the system relies on this appended technique: counterfeit requires re-mining (a highly computationally demanding operation) the block containing the modified transaction, and every subsequent block. This also means that data stored in these kinds of systems is immutable by design. The enormous computational demand, highly scattered distribution, immutability conditions, and cryptographically-secured operations, make blockchain technology a unique technical solution for storing, executing, and exchanging digital data with a high degree of security and control.

Cryptocurrency

One of the most accepted uses of blockchain technology is as payment systems. Cryptocurrency is a term comprising the blockchain qualities of circulation of tokens through cryptographically-enabled techniques. The currency label is contested, but the term was highly used to refer to blockchain-enabled endeavours, particularly in the first years of the technology. New uses for the technology contain the cryptographic and circulatory elements, but are directed towards uses beyond payment or circulation of financial assets, thus frequently referred as blockchains or distributed ledger projects. Bitcoin is considered the first cryptocurrency, although projects seeking to secure digital cash or cash-alike systems through cryptography existed before, with different degrees of success (a brief history of these experiments, and the influence they had on Bitcoin, is narrated in the third chapter of this thesis).

Hash

A hash is a representation (usually in the form of an alphanumerical string) of data. A cryptographic hash function is a mathematical operation that translate a data input into a prearranged length data output. For example, the natural language phrase “The quick brown fox jumps over the lazy dog” would become “DFCG 6HJG 0OPP Z72JF” through a hash operation. This hypothetical hash operation would drastically change the resulting hash if any minor chance is made to the original phrase, thus hashing techniques prove to be useful to detect any form of data corruption or identify a digital object (by adding, for example, a timestamp). A major advantage of hashing techniques for cryptography is that the output is not only illegible, but also that the operation to reverse engineer the original message is infeasible, and different inputs can’t share the same output. Thus, data can be compressed and remain identifiable

Mining

Mining is the operation to validate transactions, produce new tokens, and generate blocks within blockchain systems. Computers (miners) try to generate new blocks in a blockchain by appending hashes of previous blocks, hashes of bulks of transactions, timestamps, and random numbers (nonce). The difficulty of

mining consist in that the output hash has to contain a variable number of zeroes at the beginning. Since there are random numbers in the operation, mining inevitably involves multiple trial and error generation of hashes to produce an output hash with the required number of preceding zeros. The more computational power, the more chances to produce a valid hash. Therefore, mining blocks in Bitcoin is an energy and computational intensive operation (subsequent blockchains modify the variables for mining). Once a block is mined, the result is broadcasted to the network, and added to the chain, making the transactions contained in that block immutable.

PoW

A Proof-of-Work function is a computational technique to provide evidence that processing time was invested in an operation. It usually consists in generating a hash that requires a moderately hard computational work. The resultant hash is easy to check and thus serves as a convenient evidence of the average computational time/power invested. In Bitcoin and other blockchains, aggregated operations requiring PoW make the system extremely hard to temper with, yet easily verifiable.

Bibliography

'About EFF'. 2007. Electronic Frontier Foundation. 10 July 2007. https://www.eff.org/about.

Ackland, Robert, and Jamsheed Shorish. 2014. 'Political Homophily on the Web'. In *Analyzing Social Media Data and Web Networks*, 25–46. Palgrave Macmillan, London. https://doi.org/10.1057/9781137276773_2.

Agre, Philip E. 1994. 'Surveillance and Capture: Two Models of Privacy'. *The Information Society* 10 (2): 101–27. https://doi.org/10.1080/01972243.1994.9960162.

Andresen, Gavin. 2015a. 'BIP 101'. GitHub. 06 2015. https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki.

———. 2015b. 'It Must Be Done… but Is Not a Panacea'. Gavin Andresen on Svbtle. 4 May 2015. http://gavinandresen.ninja/it-must-be-done-but-is-not-a-panacea.

———. 2015c. 'Time to Roll out Bigger Blocks'. Gavin Andresen on Svbtle. 4 May 2015. http://gavinandresen.ninja/time-to-roll-out-bigger-blocks.

———. 2015d. 'Why Increasing the Max Block Size Is Urgent'. Gavin Andresen on Svbtle. 4 May 2015. http://gavinandresen.ninja/why-increasing-the-max-block-size-is-urgent.

———. 2015e. 'Will a 20MB Max Increase Centralization?' Gavin Andresen on Svbtle. 5 May 2015. http://gavinandresen.ninja/does-more-transactions-necessarily-mean-more-centralized.

———. 2016. 'A Guided Tour of the 2mb Fork'. Gavin Andresen on Svbtle. 02 2016. http://gavinandresen.ninja/a-guided-tour-of-the-2mb-fork.

Andresen, Gavin, and Mike Hearn. 2013. 'BIP 070'. GitHub. 07 2013. https://github.com/bitcoin/bips/blob/master/bip-0070.mediawiki.

Androulaki, Elli, and Ghassan O. Karame. 2014. 'Hiding Transaction Amounts and Balances in Bitcoin'. In *Trust and Trustworthy Computing*, edited by Thorsten Holz and Sotiris Ioannidis, 161–78. Lecture Notes in Computer Science 8564. Springer International Publishing. http://link.springer.com/chapter/10.1007/978-3-319-08593-7_11.

Androulaki, Elli, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. 2013. 'Evaluating User Privacy in Bitcoin'. In *Financial Cryptography and Data Security*, edited by Ahmad-Reza Sadeghi, 34–51. Lecture Notes in Computer Science 7859. Springer Berlin Heidelberg. http://link.springer.com/chapter/10.1007/978-3-642-39884-1_4.

Armitage, John. 2006. 'From Discourse Networks to Cultural Mathematics: An Interview with Friedrich A. Kittler'. *Theory, Culture & Society* 23 (7–8): 17–38. https://doi.org/10.1177/0263276406069880.

Babaioff, Moshe, Shahar Dobzinski, Sigal Oren, and Aviv Zohar. 2012. 'On Bitcoin and Red Balloons'. In *Proceedings of the 13th ACM Conference on Electronic Commerce*, 56–73. EC '12. New York, NY, USA: ACM. https://doi.org/10.1145/2229012.2229022.

Back, Adam. 2002. 'Hashcash - A Denial of Service Counter-Measure'. *Encryptopedia* (blog). 2002. http://encryptopedia.org/hashcash/.

———. 2015. 'Strongly Agree. My Suggestion 2MB Now, Then 4MB in 2 Years and 8MB in 4years Then Re-Asses. (Similar to BIP

102)Https://Twitter.Com/Jgarzik/Status/635857060626718720 …'. Microblog. *@adam3us* (blog). 25 August 2015. https://twitter.com/adam3us/status/636410827969421312.
———. n.d. 'Cypherspace'. Accessed 11 April 2014a. http://www.cypherspace.org/.
———. n.d. 'How Bitcoin Uses Hashcash'. Accessed 11 April 2014b. http://www.cypherspace.org/bitcoin/hashcash.html.
Back, Adam, G Maxwell, M Corallo, Mark Friedenbach, and L Dashjr. 2014. 'Enabling Blockchain Innovations with Pegged Sidechains'.
Backfeed.cc. 2016. 'Backfeed | Spreading Consensus'. Backfeed. 2016. http://backfeed.cc/.
'Baidu and China Telecom Stop Accepting Bitcoin, Price Slumps Again'. 2013. *CoinDesk* (blog). 7 December 2013. http://www.coindesk.com/baidu-stops-bitcoin-price-slumps-again/.
Baran, P. 1964. 'On Distributed Communications Networks'. *IEEE Transactions on Communications Systems* 12 (1): 1–9. https://doi.org/10.1109/TCOM.1964.1088883.
Barker, Davi. 2014. 'The TSA Is Looking for Bitcoin - Daily Anarchist'. Daily Anarchist. 2014. http://dailyanarchist.com/2014/02/24/the-tsa-is-looking-for-bitcoin/.
Barlow, John Perry. 1996. 'Declaration of Independence for Cyberspace'. 1996. http://wac.colostate.edu/rhetnet/barlow/barlow_declaration.html.
Barnett, George A., and Eunjung Sung. 2005. 'Culture and the Structure of the International Hyperlink Network'. *Journal of Computer-Mediated Communication* 11 (1): 217–38. https://doi.org/10.1111/j.1083-6101.2006.tb00311.x.
Barok, Dušan. 2011. 'Bitcoin: Censorship-Resistant Currency and Domain System for the People'. In *Forum American Bar Association*.
Barry, Andrew. 2001. *Political Machines: Governing a Technological Society*. A&C Black.
———. 2006. 'Technological Zones'. *European Journal of Social Theory* 9 (2): 239–53. https://doi.org/10.1177/1368431006063343.
Baumann, Annika, and Benjamin Fabianand Matthias Lischke. 2014. 'Exploring the Bitcoin Network'. In . Barcelona.
BBC. 1998. 'China to Act against "Subversives"', 18 December 1998, sec. Asia-Pacific. http://news.bbc.co.uk/1/hi/world/asia-pacific/237600.stm.
Beer, David. 2012. 'Using Social Media Data Aggregators to Do Social Research'. *Sociological Research Online* 17 (3): 10.
Beniger, James R. 1986. *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge, Mass. ; London: Harvard University Press.
Bergstra, Jan A., and Karl de Leeuw. 2013a. 'Bitcoin and Beyond: Exclusively Informational Monies'. *ArXiv:1304.4758 [Cs]*, April. http://arxiv.org/abs/1304.4758.
———. 2013b. 'Questions Related to Bitcoin and Other Informational Money'. *ArXiv:1305.5956 [Cs]*, May. http://arxiv.org/abs/1305.5956.
Bergstra, Jan A., and Peter Weijland. 2014. 'Bitcoin: A Money-like Informational Commodity'. *ArXiv:1402.4778 [Cs]*, February. http://arxiv.org/abs/1402.4778.
Berry, David. 2014. 'Post-Digital Humanities: Computation and Cultural Critique in the Arts and Humanities (EDUCAUSE Review) | EDUCAUSE.Edu'. 19 May

2014. https://www.educause.edu/ero/article/post-digital-humanities-computation-and-cultural-critique-arts-and-humanities.
Birnbaum, Michael. 2013. 'Germany Looks at Keeping Its Internet, e-Mail Traffic inside Its Borders'. *The Washington Post*, 1 November 2013. http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html.
Biryukov, Alex, Dmitry Khovratovich, and Ivan Pustogarov. 2014. 'Deanonymisation of Clients in Bitcoin P2P Network'. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 15–29. CCS '14. New York, NY, USA: ACM. https://doi.org/10.1145/2660267.2660379.
'Bitcoin Block Explorer - Blockchain.Info'. n.d. Accessed 7 May 2015. https://blockchain.info/.
'Bitcoin Cash'. n.d. Bitcoin Cash | Home. Accessed 13 September 2017. https://www.bitcoincash.org.
'Bitcoin Dice - Satoshi DICE'. n.d. Accessed 11 September 2017. https://satoshidice.com/dice.
'Bitcoin Difficulty Chart - Chart of Mining Difficulty History'. n.d. *CoinDesk* (blog). Accessed 28 September 2015. http://www.coindesk.com/data/bitcoin-mining-difficulty-time/.
'Bitcoin Obituaries: Following Bitcoin While It Dies and Rises'. 2016. *99 Bitcoins* (blog). 2016. https://99bitcoins.com/bitcoinobituaries/.
'Bitcoin Traffic Bulletin (Redux)'. n.d. Accessed 2 May 2016. http://hashingit.com/analysis/44-bitcoin-traffic-bulletin-redux.
'Bitcoin Wiki'. n.d. Accessed 18 February 2015. http://en.bitcoinwiki.org/Main_Page.
'Bitcoin/Bips'. n.d. GitHub. Accessed 2 May 2016. https://github.com/bitcoin/bips.
'Bitcoinocracy - an Opensource Project to Facilitate Decentralized Decision Making'. 2015. Reddit. 2015. https://www.reddit.com/r/Bitcoin/comments/3ef380/bitcoinocracy_an_opensource_project_to_facilitate/.
Bitcoin.org. 2015. 'Bitcoin - Open Source P2P Money'. 2015. https://bitcoin.org/en/.
Bjerg, Ole. 2016. 'How Is Bitcoin Money?' *Theory, Culture & Society* 33 (1): 53–72. https://doi.org/10.1177/0263276415619015.
Blanchette, Jean-François. 2012. *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents*. MIT Press.
Boase, Richard. 2013. 'Cypherpunks, Bitcoin & the Myth of Satoshi Nakamoto | Cybersalon'. 5 November 2013. http://www.cybersalon.org/cypherpunk/.
Bogdan, Diana. 2016. 'Benevolent Dictators and Disenchanted Believers: Bitcoin Core Developers Revisited'. 15 April 2016. http://www.coinfox.info/news/reviews/5312-benevolent-dictators-and-disenchanted-believers-bitcoin-core-developers-revisited.
Bohr, J., and M. Bashir. 2014. 'Who Uses Bitcoin? An Exploration of the Bitcoin Community'. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust (PST)*, 94–101. https://doi.org/10.1109/PST.2014.6890928.
Bradley, Arthur. 2011. 'Originary Technicity: The Theory of Technology from Marx to Derrida'.
Bratton, Benjamin H. 2016. *The Stack: On Software and Sovereignty*. 1 edition. Cambridge, Massachusetts: The MIT Press.

Brooks, Bradley, and Frank Bajak. 2013. 'Brazil Looks to Break from US-Centric Internet'. The Big Story. 17 September 2013. http://bigstory.ap.org/article/brazil-looks-break-us-centric-internet.

BtcDrak. 2015. 'BIP 105'. GitHub. 08 2015. https://github.com/bitcoin/bips/blob/master/bip-0105.mediawiki.

'Build-a-Coin Cryptocurrency Creator'. n.d. Accessed 11 September 2017. http://build-a-co.in/.

Cameron, David. 2014. 'Huge Investment in Armed Forces Means a More Secure Future for Britain', 13 July 2014. http://www.telegraph.co.uk/news/uknews/defence/10965217/Huge-investment-in-Armed-Forces-means-a-more-secure-future-for-Britain.html.

Chakraborty, Upal. 2015. 'BIP 106'. GitHub. 08 2015. https://github.com/bitcoin/bips/blob/master/bip-0106.mediawiki.

Chaum, David. 1983. 'Blind Signatures for Untraceable Payments'. In *Advances in Cryptology*, edited by David Chaum, Ronald L. Rivest, and Alan T. Sherman, 199–203. Springer US. http://link.springer.com/chapter/10.1007/978-1-4757-0602-4_18.

———. 1993. 'Numbers Can Be a Better Form of Cash than Paper'. In *Computer Security and Industrial Cryptography*, 174–78. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-57341-0_61.

'Chinese Internet Giant Baidu Starts Accepting Bitcoin'. 2013. *CoinDesk* (blog). 15 October 2013. http://www.coindesk.com/chinese-internet-giant-baidu-starts-accepting-bitcoin/.

Chun, Wendy Hui Kyong. 2008. *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*. MIT Press.

———. 2013. *Programmed Visions: Software and Memory*. Reprint edition. Cambridge, Mass.: The MIT Press.

Code, Lorraine. 2014. 'Ignorance, Injustice and the Politics of Knowledge'. *Australian Feminist Studies* 29 (80): 148–60. https://doi.org/10.1080/08164649.2014.928186.

Coeckelbergh, Prof Dr Mark. 2015. *Money Machines: Electronic Financial Technologies, Distancing, and Responsibility in Global Finance*. Surrey: Ashgate Publishing Limited.

CoinScrum and Proof of Work: Tools for the Future. 2014. https://www.youtube.com/watch?v=1Ja7HSHqt_Y&feature=youtube_gdata_player.

Corallo, Matt. 2015. '[Bitcoin-Development] Block Size Increase', 6 May 2015. https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-May/007869.html.

Courtois, Nicolas T., Marek Grajek, and Rahul Naik. 2014. 'Optimizing SHA256 in Bitcoin Mining'. In *Cryptography and Security Systems*, edited by Zbigniew Kotulski, Bogdan Księżopolski, and Katarzyna Mazur, 131–44. Communications in Computer and Information Science 448. Springer Berlin Heidelberg. http://link.springer.com/chapter/10.1007/978-3-662-44893-9_12.

Cramer, Florian. 2013. 'What Is "Post-Digital"? | Post-Digital-Research'. 14 December 2013. http://post-digital.projects.cavi.dk/?p=599.

Cusumano, M, ANDREAS Goeldi, and Dutton. 2013. 'New Businesses and New Business Models'. *W. Dutton, The Oxford Handbook of Internet*, 239–261.

Dai, Wei. 1998. 'B-Money'. 1998. http://www.weidai.com/bmoney.txt.

Dashjr, Luke. n.d. 'Bitcoin LJR'. Accessed 2 May 2016. http://luke.dashjr.org/programs/bitcoin-ljr/.
'D-CENT'. n.d. Accessed 1 May 2016. http://dcentproject.eu/.
De Filippi, Primavera. 2015. Commons Governance and Law with Primavera De Filippi Interview by Rachel O'Dwyer. http://commonstransition.org/commons-centric-law-and-governance-with-primavera-de-filippi/.
Dean, Jodi. 2002. *Publicity's Secret: How Technoculture Capitalizes on Democracy*. Cornell University Press.
Deleuze, Gilles. 1992. 'Postscript on the Societies of Control'. *October*, 3–7.
Delieb, Eric. 1971. *Matthew Boulton: Master Silversmith, 1760-1790.* New York: C.N. Potter; distributed by Crown Publishers.
Diffie, W., and M.E. Hellman. 1976. 'New Directions in Cryptography'. *IEEE Transactions on Information Theory* 22 (6): 644–54. https://doi.org/10.1109/TIT.1976.1055638.
Dourish, Paul. 2014. 'No SQL: The Shifting Materialities of Database Technology : Computational Culture'. *Computational Culture*, November. http://computationalculture.net/article/no-sql-the-shifting-materialities-of-database-technology.
DuPont, Quinn. n.d. 'The Politics of Cryptography: Bitcoin and The Ordering Machines'. *The Journal of Peer Production*. Accessed 1 January 2017. http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-politics-of-cryptography-bitcoin-and-the-ordering-machines/.
Eadicicco, Lisa. n.d. 'These Are the Most Popular IPhone Apps of 2016'. Time. Accessed 4 September 2017. http://time.com/4592864/most-popular-iphone-apps-2016/.
Elden, Stuart. 2013. *The Birth of Territory*. Chicago ; London: University of Chicago Press.
———. 2016. 'Territory'. In *The Wiley-Blackwell Companion to Human Geography*, edited by John A Agnew and James S Duncan. Vol. 15. John Wiley & Sons.
'Enciclopedia Libre Universal En Español'. 2017. Enciclopedia Libre Universal En Español. 6 June 2017. https://web.archive.org/web/20170606024300/http://enciclopedia.us.es/index.php/Enciclopedia_Libre_Universal_en_Espa%C3%B1ol.
Engels, Friedrich. 1978. 'On Authority'. In *Marx-Engels Reader*, 2nd ed., 730–33. New York: W. W. Norton and Co.
'Ethereum Project'. n.d. Accessed 11 September 2017. https://www.ethereum.org/.
Faircoin.org. 2016. 'Faircoin'. 2016. https://fair-coin.org/.
'FAQ - Bitcoin'. n.d. Accessed 9 January 2015. https://bitcoin.org/en/faq.
Finney, Hal. 2013. 'Bitcoin and Me'. 19 March 2013. http://nakamotoinstitute.org/bitcoin-and-me/.
———. n.d. 'RPOW - Reusable Proofs of Work'. Accessed 11 April 2014. http://www.finney.org/~hal/rpow/.
Fortuna, Julie, Ben Holtz, and Jocelyn Neff. 2013. 'Evolutionary Structural Analysis of the Bitcoin Network'. http://www.cryptolibrary.org/handle/21/655.
Foucault, Michel. 1980a. *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977*. Edited by Colin Gordon. 1st American Ed edition. New York: Vintage.

———. 1980b. ‘Two Lectures’. In *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977*, edited by Colin Gordon, 1st American Ed edition. New York: Vintage.
———. 1982. *The Archaeology of Knowledge: And the Discourse on Language*. New York, NY: Vintage.
———. 2012. *Discipline and Punish: The Birth of the Prison*. Vintage. Knopf Doubleday Publishing Group. https://books.google.co.uk/books?id=6rfP0H5TSmYC.
‘Free State Project’. n.d. Accessed 21 September 2017. https://freestateproject.org/about.
Fuller, Matthew. 2008. *Software Studies: A Lexicon*. MIT Press.
‘Funding of Network Security with Infinite Block Sizes’. 2013. 2013. https://bitcointalk.org/index.php?topic=157141.0;all.
Gabrys, Jennifer. 2013. *Digital Rubbish: A Natural History of Electronics*. Reprint edition. University of Michigan Press.
Galloway, Alexander R. 2004. *Protocol: How Control Exists After Decentralization*. MIT Press.
———. 2006. ‘Language Wants To Be Overlooked: On Software and Ideology’. *Journal of Visual Culture* 5 (3): 315–31. https://doi.org/10.1177/1470412906070519.
Garside, Juliette. 2015. ‘Philip Zimmermann: King of Encryption Reveals His Fears for Privacy’. *The Guardian*, 25 May 2015, sec. Technology. http://www.theguardian.com/technology/2015/may/25/philip-zimmermann-king-encryption-reveals-fears-privacy.
Garzik, Jeff. 2015. ‘BIP 102’. GitHub. 06 2015. https://github.com/bitcoin/bips/blob/master/bip-0102.mediawiki.
———. n.d. ‘BIP 109’. GitHub. Accessed 2 May 2016. https://github.com/bitcoin/bips/blob/master/bip-0102.mediawiki.
Gerlitz, Carolin, and Anne Helmond. 2013. ‘The like Economy: Social Buttons and the Data-Intensive Web’. *New Media & Society* 15 (8): 1348–65. https://doi.org/10.1177/1461444812472322.
Gloerich, Inte, and Patricia de Vries, eds. 2018. *Moneylab Reader 2: Overcoming the Hype*. Amsterdam: Institute of Network Cultures.
Goldsmith, Jack, and Tim Wu. 2008. *Who Controls the Internet?: Illusions of a Borderless World*. New York: Oxford University Press.
Golumbia, David. 2016. *The Politics of Bitcoin*. University of Minnesota Press. https://www.upress.umn.edu/book-division/books/the-politics-of-bitcoin.
Graham, Mark W. 2006. *News and Frontier Consciousness in the Late Roman Empire*. University of Michigan Press.
Greenberg, Andy. 2012. *This Machine Kills Secrets: How WikiLeakers, Hacktivists, and Cypherpunks Are Freeing the World’s Information*. Random House.
Hagelstrom, Martin. 2016. ‘Why Bitcoin’s Block Size Debate Is a Proxy War’. *CoinDesk* (blog). 12 March 2016. http://www.coindesk.com/bitcoin-block-size-proxy-war/.
Haraway, Donna. 1988. ‘Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective’. *Feminist Studies* 14 (3): 575–99. https://doi.org/10.2307/3178066.
Hardt, Michael, and Antonio Negri. 2001. *Empire*. Harvard University Press.
———. 2005. *Multitude: War and Democracy in the Age of Empire*. Penguin Books.
Hayles, N. Katherine. 2005. *My Mother Was a Computer: Digital Subjects and Literary Texts*. First Edition edition. Chicago: University Of Chicago Press.

Hearn, Mike. 2015. 'Why Is Bitcoin Forking?' Medium. 15 August 2015. https://medium.com/faith-and-future/why-is-bitcoin-forking-d647312d22c1#.4aby02bw1.

———. 2016. 'The Resolution of the Bitcoin Experiment'. Medium. 14 January 2016. https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.v7rjy8ux6.

Hern, Alex. 2015. 'Bitcoin's Forked: Chief Scientist Launches Alternative Proposal for the Currency'. *The Guardian*, 17 August 2015, sec. Technology. https://www.theguardian.com/technology/2015/aug/17/bitcoin-xt-alternative-cryptocurrency-chief-scientist.

Hiranand, Ravi. 2015. 'Exploring the Whole Galaxy of "No Man's Sky"'. CNN. 18 June 2015. http://www.cnn.com/2015/06/18/tech/no-mans-sky-sean-murray/index.html.

Hirschman, Albert O. 1970. *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States*. Harvard University Press.

'How Much Electricity Does an American Home Use? - FAQ - U.S. Energy Information Administration (EIA)'. n.d. Accessed 28 September 2015. http://www.eia.gov/tools/faqs/faq.cfm?id=97&t=3.

Hu, Tung-Hui. 2016. *A Prehistory of the Cloud*. Reprint edition. Cambridge, Massachusetts: The MIT Press.

Huckle, Steve, and Martin White. 2016. 'Socialism and the Blockchain'. *Future Internet* 8 (4): 49. https://doi.org/10.3390/fi8040049.

Hughes, Eric. 1993. 'A Cypherpunk's Manifesto'. 1993. http://www.activism.net/cypherpunk/manifesto.html.

Isaac, Benjamin. 1988. 'The Meaning of the Terms Limes and Limitanei'. *The Journal of Roman Studies* 78: 125–47. https://doi.org/10.2307/301454.

Jack, William, and Tavneet Suri. 2011. 'Mobile Money: The Economics of M-PESA'. Working Paper 16721. National Bureau of Economic Research. http://www.nber.org/papers/w16721.

Jeong, Sarah. 2013. 'The Bitcoin Protocol as Law, and the Politics of a Stateless Currency'. SSRN Scholarly Paper ID 2294124. Rochester, NY: Social Science Research Network. http://papers.ssrn.com/abstract=2294124.

Jones, Rupert. 2017. 'Cash No Longer King as Contactless Payments Soar in UK Stores'. *The Guardian*, 12 July 2017, sec. Money. http://www.theguardian.com/money/2017/jul/12/cash-contactless-payments-uk-stores-cards-british-retail-consortium.

Jong, Eduard de. 2014. 'Cash or Currency: An Overview of Electronic Payment Technology'. In . Amsterdam. http://networkcultures.org/wpmu/moneylab/2014/03/23/edward-de-jong-towards-an-open-e-currency-system/.

Jong, Eduard de, Nathaniel Tkacz, and Pablo R. Velasco. 2015. '"You Will Live as Friends and Count as Enemies": On Digital Cash and the Media of Payment.' In *Moneylab Reader: An Intervention in Digital Economy*, edited by Geert Lovink, Nathaniel Tkacz, and Patricia de Vries, 258–67. INC Reader 10. Amsterdam: Institute of Network Cultures.

Kahn, David. 1996. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Rev Sub edition. New York: Scribner.

Kaminski, Jermain, and Peter Gloor. 2014. 'Nowcasting the Bitcoin Market with Twitter Signals'. *ArXiv:1406.7577 [Cs]*, June. http://arxiv.org/abs/1406.7577.

Kant, Immanuel. 1999. *Critique of Pure Reason*. Edited by Paul Guyer and Allen W. Wood. Cambridge; New York: Cambridge University Press.
Karlstrøm, Henrik. 2014. 'Do Libertarians Dream of Electric Coins? The Material Embeddedness of Bitcoin'. *Distinktion: Scandinavian Journal of Social Theory* 15 (1): 23–36. https://doi.org/10.1080/1600910X.2013.870083.
Kelly, Kevin. 2011. *What Technology Wants*. Penguin Books.
Kelty, Christopher. 2005. 'Geeks, Social Imaginaries, and Recursive Publics'. *Cultural Anthropology* 20 (2): 185–214. https://doi.org/10.1525/can.2005.20.2.185.
Kirschenbaum, Matthew. 2007. *Mechanisms: New Media and the Forensic Imagination*. MIT Press. https://mitpress.mit.edu/books/mechanisms.
Kitchin, Rob. 2014. 'Thinking Critically About and Researching Algorithms'. SSRN Scholarly Paper ID 2515786. Rochester, NY: Social Science Research Network. http://papers.ssrn.com/abstract=2515786.
Kitchin, Rob, and Martin Dodge. 2011. *Code/Space: Software and Everyday Life*. MIT Press.
Kittler, Friedrich A. 1999. *Gramophone, Film, Typewriter*. Translated by Geoffrey Winthrop-Young and Michael Wutz. 1 edition. Stanford, Calif: Stanford University Press.
———. 2008. 'Code (or, How You Can Write Something Differently)'. In *Software Studies: A Lexicon*, by Matthew Fuller. MIT Press.
Kittler, Friedrich A., and Michael Metteer. 1992. *Discourse Networks, 1800/1900*. 1 edition. Stanford, Calif: Stanford University Press.
Kondor, Dániel, Márton Pósfai, István Csabai, and Gábor Vattay. 2014. 'Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network'. *PLoS ONE* 9 (2): e86197. https://doi.org/10.1371/journal.pone.0086197.
Krämer, Sybille. 2015. *Medium, Messenger, Transmission: An Approach to Media Philosophy*. Amsterdam University Press.
Lamport, Leslie, Robert Shostak, and Marshall Pease. 1982. 'The Byzantine Generals Problem'. *ACM Trans. Program. Lang. Syst.* 4 (3): 382–401. https://doi.org/10.1145/357172.357176.
Lash, Scott. 2007. 'Power after Hegemony Cultural Studies in Mutation?' *Theory, Culture & Society* 24 (3): 55–78. https://doi.org/10.1177/0263276407075956.
Latour, Bruno. 1996. *Aramis, or, The Love of Technology*. Harvard University Press.
———. 2007a. *Reassembling the Social: An Introduction to Actor-Network-Theory*. OUP Oxford.
———. 2007b. 'Turning Around Politics: A Note on Gerard de Vries' Paper'. *Social Studies of Science* 37 (5): 811–20. https://doi.org/10.1177/0306312707081222.
Law, John, and Evelyn Ruppert. 2013. 'The Social Life Of Methods: Devices'. *Journal of Cultural Economy* 6 (3): 229–40. https://doi.org/10.1080/17530350.2013.812042.
Lessig, Lawrence. 2006. *Code: And Other Laws of Cyberspace, Version 2.0*. 2nd Revised ed. edition. New York: Basic Books.
Levchenko, Kirill, Vacha Dave, Stefan Savage, Alex C. Snoeren, Damon McCoy, Chris Grier, Hitesh Dharmdasani, Sarah Meiklejohn, Danny Yuxing Huang, and Nicholas Weaver. 2014. 'Botcoin: Monetizing Stolen Cycles'. *Internet Society NDSS 2014*. http://www.cryptolibrary.org/handle/21/434.
Levy, Steven. 1996. 'Crypto Rebels'. In *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, by Peter Ludlow, 185–206. MIT Press.

Lightbody, Brian. 2010. *Philosophical Genealogy: An Epistemological Reconstruction of Nietzsche and Foucault's Genealogical Method*. Peter Lang.
'List of Bitcoin Services That Support/Oppose Increasing Max Block Size'. n.d. Reddit. Accessed 2 May 2016. https://www.reddit.com/r/Bitcoin/comments/37y8wm/list_of_bitcoin_services_that_supportoppose/.
Litecoin.org. 2015. 'Litecoin - Open Source P2P Digital Currency'. 2015. https://litecoin.org/.
López, Julio, and Ricardo Dahab. 2000. 'An Overview of Elliptic Curve Cryptography'.
Lovink, Geert, Nathaniel Tkacz, and Patricia de Vries. 2015. *Moneylab Reader : An Intervention in Digital Economy*. Amsterdam: Institute of Network Cultures.
Lovink, Geert, and Soenke Zehle. 2005. *Incommunicado Reader*. Institute of Network Cultures.
Lucas, George. 1978. *Star Wars: Episode IV - A New Hope*. Action, Adventure, Fantasy. http://www.imdb.com/title/tt0076759/.
Luhmann, Niklas. 1975. *Legitimation durch Verfahren*. Luchterhand.
Lupton, Deborah. 2014. *Digital Sociology*. Routledge.
Lury, Celia, and Nina Wakeford. 2012a. 'Introduction: A Perpetual Inventory'. In *Inventive Methods: The Happening of the Social*, 1–25. Routledge.
———. 2012b. *Inventive Methods: The Happening of the Social*. Routledge.
Lyotard, Jean-François. 1984. *The Postmodern Condition: A Report on Knowledge*. University of Minnesota Press.
Mackenzie, Adrian, and Ruth McNally. 2013. 'Living Multiples: How Large-Scale Scientific Data-Mining Pursues Identity and Differences'. *Theory, Culture & Society* 30 (4): 72–91. https://doi.org/10.1177/0263276413476558.
Malone, D., and K.J. O'Dwyer. 2014. 'Bitcoin Mining and Its Energy Footprint'. In , 280–85. Institution of Engineering and Technology. https://doi.org/10.1049/cp.2014.0699.
Manovich, Lev. 2001. *The Language of New Media*. MIT Press.
Marres, Noortje. 2007. 'The Issues Deserve More Credit: Pragmatist Contributions to the Study of Public Involvement in Controversy'. *Social Studies of Science* 37 (5): 759–80. https://doi.org/10.1177/0306312706077367.
———. 2012. 'The Redistribution of Methods: On Intervention in Digital Social Research, Broadly Conceived'. *The Sociological Review* 60: 139–65. https://doi.org/10.1111/j.1467-954X.2012.02121.x.
———. 2015. 'Why Map Issues? On Controversy Analysis as a Digital Method'. *Science, Technology & Human Values*, 0162243915574602.
Marres, Noortje, and Esther Weltevrede. 2013. 'Scraping the Social? Issues in Live Social Research'. *Journal of Cultural Economy* 6 (3): 313–335.
Marx, Karl. 1980. *Grundrisse*. Translated by David McLellan. 2nd ed. London (etc.): Macmillan.
———. 1992. *Capital: Volume 1: A Critique of Political Economy*. Edited by Ernest Mandel. Translated by Ben Fowkes. Reprint edition. London ; New York, N.Y: Penguin Classics.
massobs.org.uk. 2015. 'Mass Observation Project'. 2015. http://www.massobs.org.uk/about/mass-observation-project.
Matonis, Jon. n.d. 'Bitcoin Foundation Launches To Drive Bitcoin's Advancement'. Forbes. Accessed 18 September 2017.

https://www.forbes.com/sites/jonmatonis/2012/09/27/bitcoin-foundation-launches-to-drive-bitcoins-advancement/.
Maurer, Bill. 2014. *Closed Loops and Private Gateways: Money, Technology and the Public Interest in Payment (MoneyLab)*. http://vimeo.com/90207123.
Maurer, Bill, Taylor C. Nelms, and Lana Swartz. 2013. '"When Perhaps the Real Problem Is Money Itself!": The Practical Materiality of Bitcoin'. *Social Semiotics* 23 (2): 261–77. https://doi.org/10.1080/10350330.2013.777594.
May, Timothy C. 1994. 'Cyphernomicon'. 1994. http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html.
———. 1996. 'A Crypto Anarchist Manifesto'. In *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, by Peter Ludlow, 237–40. MIT Press.
Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. 2013. 'A Fistful of Bitcoins: Characterizing Payments Among Men with No Names'. In *Proceedings of the 2013 Conference on Internet Measurement Conference*, 127–140. IMC '13. New York, NY, USA: ACM. https://doi.org/10.1145/2504730.2504747.
Merkle, Ralph C. 1980. 'Protocols for Public Key Cryptosystems'. In *Null*, 122. IEEE.
Mersch, Yves. n.d. 'ECB: Euro Banknotes – a Means of Payment Recognised Worldwide'. Accessed 30 July 2014. https://www.ecb.europa.eu/press/key/date/2014/html/sp140519.en.html.
Mitchell, William J. 1996. *City of Bits: Space, Place, and the Infobahn*. Revised ed. edition. Cambridge, Mass.: The MIT Press.
Mittal, Sonal. 2012. 'Is Bitcoin Money? Bitcoin and Alternate Theories of Money'. SSRN Scholarly Paper ID 2434194. Rochester, NY: Social Science Research Network. http://papers.ssrn.com/abstract=2434194.
Moor, Liz, and Emma Uprichard. 2014. 'The Materiality of Method: The Case of the Mass Observation Archive'. *Sociological Research Online* 19 (3): 10.
Morozov, Evgeny. 2013. *To Save Everything, Click Here: The Folly of Technological Solutionism*. PublicAffairs.
Moser, M., R. Bohme, and D. Breuker. 2013. 'An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem'. In *ECrime Researchers Summit (ECRS), 2013*, 1–14. https://doi.org/10.1109/eCRS.2013.6805780.
Mouffe, Chantal. 2000. 'Deliberative Democracy or Agonistic Pluralism'. IHS Series. December 2000. http://irihs.ihs.ac.at/1312/.
Mu, Eric. 2015. 'My Life Inside a Remote Chinese Bitcoin Mine'. *CoinDesk* (blog). 8 June 2015. http://www.coindesk.com/my-life-inside-a-remote-chinese-bitcoin-mine/.
Nakamoto, Satoshi. 2008a. 'CML: Bitcoin P2P e-Cash Paper'. Archive. Cryptography Mailing List. 2008. https://www.mail-archive.com/cryptography%40metzdowd.com/msg09959.html.
———. 2008b. 'Bitcoin: A Peer-to-Peer Electronic Cash System', October. https://bitcoin.org/bitcoin.pdf.
'Nasdaq Linq Enables First-Ever Private Securities Issuance Documented With Blockchain Technology (NASDAQ:NDAQ)'. n.d. Accessed 16 September 2016. http://ir.nasdaq.com/releasedetail.cfm?ReleaseID=948326.
Nassehi, Armin. 2017. 'Society Throught the Lens of the Digital (Keynote)'. In *Herrenhausen Conference*. Hannover.
Negri, Antonio. 1991. *The Savage Anomaly: The Power of Spinoza's Metaphysics and Politics*. U of Minnesota Press.

‘NY Financial Regulator Lawsky Releases Final BitLicense Rules for Bitcoin Firms - WSJ’. n.d. Accessed 5 September 2017. https://www.wsj.com/articles/ny-financial-regulator-lawsky-releases-final-bitlicense-rules-for-bitcoin-firms-1433345396.

O’Dwyer, Rachel. 2012. ‘This Is Not a Bit-Pipe: A Political Economy of the Substrate Network’. *Fibreculture Journal* 20 (June). http://twenty.fibreculturejournal.org/2012/06/18/fcj-138-this-is-not-a-bit-pipe-a-political-economy-of-the-substrate-network/.

———. 2015. ‘The Revolution Will (Not) Be Decentralised: Blockchains’. *Commons Transition* (blog). 11 June 2015. http://commonstransition.org/the-revolution-will-not-be-decentralised-blockchains/.

Parikka, Jussi. 2012. *What Is Media Archaeology*. Polity.

———. 2014. ‘Cultural Techniques of Cognitive Capitalism: Metaprogramming and the Labour of Code’. *Cultural Studies Review* 20 (1): 30–52. https://doi.org/10.5130/csr.v20i1.3831.

Pariser, Eli. 2011. *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*. Penguin UK.

Parisi, Luciana. 2013. *Contagious Architecture*. MIT Press. https://mitpress.mit.edu/books/contagious-architecture.

Pasquinelli, Matteo. 2017. ‘Arcana Mathematica Imperii: The Evolution of Western Computational Norms’. In *Former West*, by Maria Hlavajova. Boston, MA: MIT Press. https://www.academia.edu/26313149/Arcana_Mathematica_Imperii_The_Evolution_of_Western_Computational_Norms.

Paul, Kari. 2015. ‘Bitcoin Mining in an Abandoned Iowa Grocery Store’. Motherboard. 17 July 2015. http://motherboard.vice.com/read/bitcoin-mining-in-an-abandoned-iowa-grocery-store.

Popper, Nathaniel. 2015. *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. New York, NY: Harper.

———. 2016. ‘A Bitcoin Believer’s Crisis of Faith’. *The New York Times*, 14 January 2016. http://www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html.

Puckett, Jim, and Ted Smith, eds. 2003. *Exporting Harm: The High-Tech Trashing of Asia*. Seattle, Wash.: Diane Pub Co.

Raymond, Eric S. 2008. *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. O’Reilly Media, Inc.

———. n.d. ‘Homesteading the Noosphere’. Accessed 11 September 2017. http://www.catb.org/~esr/writings/cathedral-bazaar/homesteading/.

Redshaw, Thomas. 2017. ‘Bitcoin beyond Ambivalence: Popular Rationalization and Feenberg’s Technical Politics’. *Thesis Eleven* 138 (1): 46–64. https://doi.org/10.1177/0725513616689390.

Reid, Fergal, and Martin Harrigan. 2013. ‘An Analysis of Anonymity in the Bitcoin System’. In *Security and Privacy in Social Networks*, edited by Yaniv Altshuler, Yuval Elovici, Armin B. Cremers, Nadav Aharony, and Alex Pentland, 197–223. Springer New York. http://link.springer.com/chapter/10.1007/978-1-4614-4139-7_10.

Rivest, R. L., A. Shamir, and L. Adleman. 1978. ‘A Method for Obtaining Digital Signatures and Public-Key Cryptosystems’. *Commun. ACM* 21 (2): 120–126. https://doi.org/10.1145/359340.359342.

Rizzo, Pete. 2014. ‘Blockstream: $21 Million Funding Will Drive Bitcoin Development’. *CoinDesk* (blog). 18 November 2014.

http://www.coindesk.com/blockstream-21-million-funding-will-drive-bitcoin-development/.
Roberts, Daniel. n.d. 'Why a Slew of Bitcoin Startups Fled New York'. Fortune. Accessed 5 September 2017. http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/.
Rogers, Richard. 2009. *The End of the Virtual: Digital Methods*. Amsterdam: Vossiuspers UvA.
———. 2012. 'Mapping and the Politics of Web Space'. *Theory, Culture & Society* 29 (4–5): 193–219. https://doi.org/10.1177/0263276412450926.
———. 2013. *Digital Methods*. MIT Press.
Ruppert, Evelyn, John Law, and Mike Savage. 2013. 'Reassembling Social Science Methods: The Challenge of Digital Devices'. *Theory, Culture & Society* 30 (4): 22–46.
Sachy, Marco. 2015. 'Blockchain for the Social Good | Nesta'. 10 June 2015. http://www.nesta.org.uk/blog/blockchain-social-good.
Sack, Robert David. 1986. *Human Territoriality: Its Theory and History*. CUP Archive.
Sanchez, Washington. 2015. 'BIP 107'. GitHub. 09 2015. https://github.com/bitcoin/bips/blob/master/bip-0107.mediawiki.
Sassen, Saskia. 2002. 'Towards a Sociology of Information Technology'. *Current Sociology* 50 (3): 365–88. https://doi.org/10.1177/0011392102050003005.
———. 2006. *Territory, Authority, Rights: From Medieval to Global Assemblages*. Princeton University Press.
Saxena, Amitabh, Janardan Misra, and Aritra Dhar. 2014. 'Increasing Anonymity in Bitcoin'. In *Financial Cryptography and Data Security*, edited by Rainer Böhme, Michael Brenner, Tyler Moore, and Matthew Smith, 122–39. Lecture Notes in Computer Science 8438. Springer Berlin Heidelberg. http://link.springer.com/chapter/10.1007/978-3-662-44774-1_9.
'Scalability Debate Continues As Bitcoin XT Proposal Stalls'. 2016. CoinDesk. 11 January 2016. https://www.coindesk.com/scalability-debate-bitcoin-xt-proposal-stalls/.
Scholz, Trebor, and Nathan Schneider. 2017. *Ours to Hack and to Own*. New York.
SCI-Arc Channel. 2016. *Benjamin H. Bratton Interview*. https://www.youtube.com/watch?v=W8My0aLsIMA.
Scott, Brett. 2014. 'Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain'. *E-International Relations* (blog). 2014. http://www.e-ir.info/2014/06/01/visions-of-a-techno-leviathan-the-politics-of-the-bitcoin-blockchain/.
———. 2016a. 'How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?' UNRISD Working Paper.
———. 2016b. 'The War on Cash'. *The Long and Short*, 19 August 2016. war-on-cash.html.
Selgin, George. 2015. 'Synthetic Commodity Money'. *Journal of Financial Stability*, Special Issue: Instead of the Fed: Past and Present Alternatives to the Federal Reserve System, 17 (April): 92–99. https://doi.org/10.1016/j.jfs.2014.07.002.
Shah, D., and Kang Zhang. 2014. 'Bayesian Regression and Bitcoin'. In *2014 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 409–14. https://doi.org/10.1109/ALLERTON.2014.7028484.
Siegel, Matt. 2016. 'Upstart Australian Political Party Wants to Use Bitcoin as Basis for Governance Style'. 16 February 2016.

http://www.rawstory.com/2016/02/upstart-australian-political-party-wants-to-use-bitcoin-as-basis-for-governance-style/.
Simonite, Tom. 2014. 'Meet Gavin Andresen, the Most Powerful Person in the World of Bitcoin'. MIT Technology Review. 15 August 2014. https://www.technologyreview.com/s/527051/the-man-who-really-built-bitcoin/.
Smith, Adam. 1791. *An Inquiry Into the Nature and Causes of the Wealth of Nations: By Adam Smith*, ... J. J. Tourneisen; and J. L. Legrand.
Smyth, Lui. 2014a. 'The Politics of Bitcoin'. *Simulacrum* (blog). 7 March 2014. https://spacedruiddotcom.wordpress.com/2014/03/07/the-politics-of-bitcoin/.
———. 2014b. 'Trust, Organisation, and Community Within Bitcoin'. *Simulacrum* (blog). 2 April 2014. https://spacedruiddotcom.wordpress.com/2014/04/02/bitcoin-trust/.
'Soft Block Size Limit Reached, Action Required by YOU'. 2013. 2013. https://bitcointalk.org/index.php?topic=149668.0;all.
Southurst, Jon. 2014. 'Australian Government: Welfare Applicants Must Declare Bitcoin Assets'. *CoinDesk* (blog). 14 November 2014. http://www.coindesk.com/australian-government-welfare-applicants-must-declare-bitcoin-assets/.
Spencer, Leon. 2015. 'Australia's CoinJar Moves HQ to UK for "progressive" Bitcoin Scene'. ZDNet. 2015. http://www.zdnet.com/article/australias-coinjar-moves-hq-to-uk-for-progressive-bitcoin-scene/.
Srnicek, Nick. 2016. *Platform Capitalism*. 1 edition. Cambridge, UK ; Malden, MA: Polity.
Stengers, Isabelle. 2010. *Cosmopolitics I*. Translated by Robert Bononno. Minneapolis: Univ Of Minnesota Press.
Stephens, Monica. 2012. 'Featured Graphic: Digital Divide: The Geography of Internet Access'. *Environment and Planning A* 44: 1009–1010.
Stokes, Robert. 2012. 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar'. *Information & Communications Technology Law* 21 (3): 221–36. https://doi.org/10.1080/13600834.2012.744225.
Sun, Leo. 2017. 'Facebook Inc.'s WhatsApp Hits 900 Million Users: What Now? -'. The Motley Fool. 2017. https://www.fool.com/investing/general/2015/09/11/facebook-incs-whatsapp-hits-900-million-users-what.aspx.
Sunstein, Cass R. 2009. *Republic.Com 2.0*. Princeton University Press.
Surda, Peter. 2012. 'Economics of Bitcoin Is Bitcoin an Alternative to Fiat Currencies and Gold'. http://www.cryptolibrary.org/handle/21/625.
Swartz, Lana. 2017. 'Blockchain Dreams: Imagining Techno-Economic Alternatives After Bitcoin'. In *Another Economy Is Possible: Culture and Economy in a Time of Crisis*, 1 edition. Malden, MA: Polity.
Szabo, Nick. 2002. 'Shelling Out -- The Origins of Money'. 2002. http://szabo.best.vwh.net/shell.html.
———. 2005. 'Bit Gold'. *Unenumerated* (blog). December 2005. http://unenumerated.blogspot.de/2005/12/bit-gold.html.
———. 2011. 'Bitcoin, What Took Ye so Long?' Blog. *Unenumerated* (blog). 28 May 2011. http://unenumerated.blogspot.co.uk/2011/05/bitcoin-what-took-ye-so-long.html.
Taaki, Amir. n.d. 'BIP 001'. GitHub. Accessed 2 May 2016. https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki.

Terranova, Tiziana. 2014. ‘Red Stack Attack! Algorithms, Capital, and the Automation of the Common’. *Quaderni Di San Precario, February* 14.
Terranova, Tiziana, and Andrea Fumagalli. 2015. ‘Financial Capital and the Money of the Common: The Case of Commoncoin’. In *Moneylab Reader: An Intervention in Digital Economy*. INC Reader 10. Amsterdam.
The Law Library of Congress. 2016. ‘Regulation of Bitcoin in Selected Jurisdictions (Web Updates)’. Web page. September 2016. https://loc.gov/law/help/bitcoin-survey/.
‘The Tao of IETF: A Novice’s Guide to the Internet Engineering Task Force’. 2012. August 2012. https://www.ietf.org/tao.html.
Tkacz, Nathaniel. 2011. ‘The Politics of Forking Paths’. In *Critical Point of View : A Wikipedia Reader*, edited by Geert Lovink and Nathaniel Tkacz, 94–109. Amsterdam: Institute of Network Cultures. http://networkcultures.org/wpmu/portal/publications/inc-readers/critical-point-of-view-a-wikipedia-reader/.
———. 2015. *Wikipedia and the Politics of Openness*. University of Chicago Press. http://www.press.uchicago.edu/ucp/books/book/chicago/W/bo19085555.html.
Toor, Amar. 2013. ‘Will the Global NSA Backlash Break the Internet?’ The Verge. 8 November 2013. http://www.theverge.com/2013/11/8/5080554/nsa-backlash-brazil-germany-raises-fears-of-internet-balkanization.
Vasek, Marie, Micah Thornton, and Tyler Moore. 2014. ‘Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem’. In *Financial Cryptography and Data Security*, edited by Rainer Böhme, Michael Brenner, Tyler Moore, and Matthew Smith, 57–71. Lecture Notes in Computer Science 8438. Springer Berlin Heidelberg. http://link.springer.com/chapter/10.1007/978-3-662-44774-1_5.
Verbücheln, Stephan. 2015. ‘How Perfect Offline Wallets Can Still Leak Bitcoin Private Keys’. *ArXiv:1501.00447 [Cs]*, January. http://arxiv.org/abs/1501.00447.
Vigna, Paul. 2016. ‘Bitcoin Startup Blockstream Raises $55 Million in Funding Round’. *Wall Street Journal*, 3 February 2016, sec. Markets. http://www.wsj.com/articles/bitcoin-startup-blockstream-raises-55-million-in-funding-round-1454518655.
Vries, Gerard de. 2007. ‘What Is Political in Sub-Politics?: How Aristotle Might Help STS’. *Social Studies of Science* 37 (5): 781–809. https://doi.org/10.1177/0306312706070749.
Wallace, Benjamin. n.d. ‘The Rise and Fall of Bitcoin’. WIRED. Accessed 21 September 2017. https://www.wired.com/2011/11/mf_bitcoin/.
Wandery, Oscar. 2014. *Bitcoin: A Seemingly Rampant Elevator, or Is Someone Pushing Its Buttons? : A Case Study on Bitcoin’s Fluctuations in Price and Concept*. http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A740506&dswid=-853.
Weber, Max. 1991. ‘Politics as Vocation’. In *From Max Weber: Essays in Sociology*. Psychology Press.
Weber, Steve. 2004. *The Success of Open Source*. Harvard University Press.
Welch, Chris. 2017. ‘Facebook Crosses 2 Billion Monthly Users’. The Verge. 27 June 2017. https://www.theverge.com/2017/6/27/15880494/facebook-2-billion-monthly-users-announced.
Wellman, Barry. 2004. ‘The Three Ages of Internet Studies: Ten, Five and Zero Years Ago’. *New Media & Society* 6 (1): 123–29. https://doi.org/10.1177/1461444804040633.

WeUseCoins. 2014. *What Is Bitcoin? (V2)*. https://www.youtube.com/watch?v=Gc2en3nHxA4&feature=youtu.be.

Winner, Langdon. 1980. 'Do Artifacts Have Politics?' *Daedalus* 109 (1): 121–136.

Wirdum, Aaron van. 2015. 'Chinese Mining Pools Propose Alternative 8 MB Block Size'. CoinTelegraph. 16 June 2015. http://cointelegraph.com/news/chinese-mining-pools-propose-alternative-8-mb-block-size.

Wuille, Pieter. 2015. 'BIP 103'. GitHub. 07 2015. https://github.com/bitcoin/bips/blob/master/bip-0103.mediawiki.

Wynn, Jonathan R. 2009. 'Digital Sociology: Emergent Technologies in the Field and the Classroom'. In *Sociological Forum*, 24:448–456. Wiley Online Library., 24:448–456. Wiley Online Library.