INTERNET POLICY REVIEW
Journal on internet regulation

Volume 5 | Issue 3

The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure

Primavera De Filippi
Berkman Klein Center for Internet & Society, Harvard University, United States

Benjamin Loveluck
Télécom ParisTech (Université Paris-Saclay) and CERSA (CNRS-Paris 2), France, benjamin.loveluck@telecom-paristech.fr

Published on 30 Sep 2016 | DOI: 10.14763/2016.3.427

Abstract: Bitcoin is a decentralised currency and payment system that seeks to eliminate the need for trusted authorities. It relies on a peer-to-peer network and cryptographic protocols to perform the functions of traditional financial intermediaries, such as verifying transactions and preserving the integrity of the system. This article examines the political economy of Bitcoin, in light of a recent dispute that divided the Bitcoin community with regard to a seemingly simple technical issue: whether or not to increase the block size of the Bitcoin blockchain. By looking at the socio-technical constructs of Bitcoin, the article distinguishes between two distinct coordination mechanisms: governance by the infrastructure (achieved via the Bitcoin protocol) and governance of the infrastructure (managed by the community of developers and other stakeholders). It then analyses the invisible politics inherent in these two mechanisms, which together display a highly technocratic power structure. On the one hand, as an attempt to be self-governing and self-sustaining, the Bitcoin network exhibits a strong market-driven approach to social trust and coordination, which has been embedded directly into the technical protocol. On the other hand, despite being an open source project, the development and maintenance of the Bitcoin code ultimately relies on a small core of highly skilled developers who play a key role in the design of the platform.

Keywords: Bitcoin, Blockchain, Peer-to-peer (P2P)

Article information

Received: 05 May 2016 **Reviewed:** 17 Jun 2016 **Published:** 30 Sep 2016
Licence: Creative Commons Attribution 3.0 Germany
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure

Citation: De Filippi, P. & Loveluck, B. (2016). The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. *Internet Policy Review*, 5(3). DOI: 10.14763/2016.3.427

This paper is part of 'Doing internet governance: practices, controversies, infrastructures, and

institutions', a Special issue of the Internet Policy Review.

INTRODUCTION

Since its inception in 2008, the grand ambition of the Bitcoin project has been to support direct monetary transactions among a network of peers, by creating a decentralised payment system that does not rely on any intermediaries. Its goal is to eliminate the need for trusted third parties, particularly central banks and governmental institutions, which are prone to corruption.

Recently, the community of developers, investors and users of Bitcoin has experienced what can be regarded as an important *governance crisis* – a situation whereby diverging interests have run the risk of putting the whole project in jeopardy. This governance crisis is revealing of the limitations of excessive reliance on technological tools to solve issues of social coordination and economic exchange. Taking the Bitcoin project as a case study, we argue that online peer-to-peer communities involve inherently political dimensions, which cannot be dealt with purely on the basis of protocols and algorithms.

The first part of this paper exposes the specificities of Bitcoin, presents its underlying political economy, and traces the short history of the project from its inception to the crisis. The second part analyses the governance structure of Bitcoin, which can be understood as a two-layered construct: an *infrastructure* seeking to govern user behaviour via a decentralised, peer-to-peer network on the one hand, and an *open source community of developers* designing and architecting this infrastructure on the other. We explore the challenges faced at both levels, the solutions adopted to ensure the sustainability of the system, and the unacknowledged power structures they involve. In a third part, we expose the *invisible politics* of Bitcoin, with regard to both the implicit assumptions embedded in the technology and the highly centralised and largely undemocratic development process it relies on. We conclude that the overall system displays a highly technocratic power structure, insofar as it is built on automated technical rules designed by a minority of experts with only limited accountability for their decisions. Finally, drawing on the wider framework of internet governance research and practice, we argue that some form of social institution may be needed to ensure accountability and to preserve the legitimacy of the system as a whole – rather than relying on technology alone.

I. BITCOIN IN THEORY AND PRACTICE

A. THE BITCOIN PROJECT: POLITICAL ECONOMY OF A TRUSTLESS PEER-TO-PEER NETWORK

Historically, money has taken many different forms. Far from being an exclusively economic tool, money is closely associated with social and political systems as a whole – which Nigel Dodd refers to as *the social life of money* (Dodd 2014). Indeed, money has often been presented as an instrument which can be leveraged to shape society in certain ways and as Dodd has shown, this includes powerful utopian dimensions: for sociologist Georg Simmel for instance, an ideal social order hinged upon the definition of a "perfect money" (Simmel, 2004). In the wake of economic crises in particular, it is not uncommon to witness the emergence of alternative money or exchange frameworks aimed at establishing different social relations between individuals – more egalitarian, or less prone to accumulation and speculation (North, 2007). On the other hand however, ideals of self-regulating markets have often sought to *detach* money from

existing social relations, resulting in a progressive "disembedding" of commercial interactions from their social and cultural context (Polanyi, 2001 [1944]).

Since it first appeared in 2009, the decentralised cryptocurrency Bitcoin has raised high hopes for its potential to reshuffle not only the institutions of banking and finance, but also more generally power relations within society. The potential consequences of this innovation, however, are profoundly ambivalent. On the one hand, Bitcoin can be presented as a neoliberal project insofar as it radicalises Friedrich Hayek's and Milton Friedman's ambition to end the monopoly of nation-states (via their central banks) on the production and distribution of money (Hayek, 1990), or as a *libertarian dream* which aims at reducing the control of governments on the economy (De Filippi, 2014). On the other hand, it has also been framed as a solution for greater social justice, by undermining oligopolistic and anti-democratic arrangements between big capital and governments, which are seen to favour economic crises and inequalities. Both of these claims hinge on the fact that as a socio-technical assemblage, Bitcoin seems to provide a solution for "governing without governments", which appeals to liberal sentiments both from the left and from the right. Its implicit political project can therefore be understood as effectively getting rid of politics by relying on technology.

More generally, distributed networks have long been associated with a redistribution of power relations, due to the elimination of single points of control. This was one of the main interpretations of the shift in telecommunications routing methods from circuit switching to packet switching in the 1960s and the later deployment of the internet protocol suite (TCP/IP) from the 1970s onwards (Abbate, 1999), as well as the adoption of the end-to-end principle – which proved to be a compelling but also partly misleading metaphor (Gillespie, 2006). The idea was that information could flow through multiple and unfiltered channels, thus circumventing any attempts at controlling or censoring it, and providing a basis for more egalitarian social relations as well as stronger privacy. In practice however, it became clear that network design is much more complex and that additional software, protocols and hardware, at various layers of the network, could (and did) provide alternate forms of re-centralisation and control and that, moreover, the internet was not structurally immune to other modes of intervention such as law and regulation (Benkler, 2016).

However, there have been numerous attempts at *re-decentralising* the network, most of which have adopted peer-to-peer architectures as opposed to client-server alternatives, with the underlying assumption that such technical solutions provide both individual freedom and "a promise of equality" (Agre, 2003) [1]. Other technologies have also been adopted in order to add features relating to user privacy for instance, which involve alternative routing methods (Dingledine, Mathewson, & Syverson, 2004) and cryptography (which predates computing, see e.g. Kahn 1996). In particular, such ideas were strongly advocated starting from the late 1980s by an informal collective of hackers, mathematicians, computer scientists and activists known as *cypherpunks*, who saw strong cryptography as a means of achieving greater privacy and security of interpersonal communications, especially in the face of perceived excesses and abuses on the part of governmental authorities. [2] Indeed, all of these solutions pursue implicit or explicit goals, in terms of their social or political consequences, which can be summed up as enabling self-organised direct interactions between individuals, without relying on a third party for coordination, and also preventing any form of surveillance or coercion.

Yet cryptography is not only useful to protect the privacy of communications; it can also serve as a means to promote further decentralisation and disintermediation when combined with a peer-to-peer architecture. In 2008, a pseudonymous entity named Satoshi Nakamoto released a

white paper on the Cryptography Mailing list (metzdowd.com) describing the idea of a decentralised payment system relying on a distributed ledger with cryptographic primitives (Nakamoto, 2008a). One year later, a first implementation of the ideas defined in the white paper was released and the Bitcoin network was born. It introduces its own native currency (or unit of account) with a fixed supply – and whose issuance is regulated, only and exclusively, by technological means. The Bitcoin network can therefore be used to replace at least some of the key functions played by central banks and other financial institutions in modern societies: the issuance of money on the one hand, and, on the other hand, the fiduciary functions of banks and other centralised clearing houses.

Supported by many self-proclaimed libertarians, Bitcoin is often presented as an alternative monetary system, capable of bypassing most of the state-backed financial institutions – with all of their shortcomings and vested interests which have become so obvious in the light of the financial crisis of 2008. Indeed, as opposed to traditional centralised economies, Bitcoin's monetary supply is not controlled by any central authority, but is rather defined (in advance) by the Bitcoin protocol – which precisely stipulates the total amount of bitcoins that will ever come into being (21 million) and the rate at which they will be issued over time. A certain number of bitcoins are generated, on average, every ten minutes and assigned as a reward to those who lend their computational resources to the Bitcoin network in order to both operate and secure the network. In this sense, Bitcoin can be said to mimic the characteristics of gold. Just as gold cannot be created out of thin air, but rather needs to be extracted from the earth (through mining), Bitcoin also requires a particular kind of computational effort – also known as *mining* – in order for the network protocol to generate new bitcoins (and just as gold progressively becomes harder to find as the stock gets depleted over, also the amount of bitcoins generated through mining decreases over time).

The establishment and maintenance of a currency has traditionally been regarded as a key prerogative of the State, as well as a central institution of democratic societies. Controlling the money supply, by different means, is one of the main instruments that can be leveraged in order to shape the economy, both domestically and in the context of international trade. Yet, regardless of whether one believes that the State has the right (or duty) to intervene in order to regulate the market economy, monetary policies have sometimes been instrumentalised by certain governments using inflation as a means to finance government spending (e.g. in the case of the Argentine great depression of 1998-2002). Perhaps most critical is the fact that, with the introduction of fractional-reserve banking, commercial banks acquired the ability to (temporarily) increase the money supply by giving out loans which are not backed up by actual funds (Ferguson, 2008). [3] The fractional-reserve banking system (and the tendency of commercial banks to create money at unsustainable rates) is believed to be one of the main factors leading to the global financial crisis of 2008 – which has brought the issue of private money issuance back into the public debate (Quinn, 2009).

Although there have been many attempts at establishing alternative currencies, and cryptocurrencies have also been debated for a long time, the creation of the Bitcoin network was in large part motivated in response to the social and cultural contingencies that emerged during the global financial crisis of 2008. As explicitly stated by Satoshi Nakamoto in various blog posts and forums, Bitcoin aimed at eradicating corruption from the realm of currency issuance and exchange. Given that governments and central banks could no longer be trusted to secure the value of fiat currency and other financial instruments, Bitcoin was designed to operate as a *trustless* technology, which only relies on maths and cryptography. [4] The paradox being that this *trustless technology* is precisely what is needed for building a new form of "distributed trust"

(Mallard, Méadel, & Musiani, 2014).

Trust management is a classic issue in peer-to-peer computing, and can be understood as *the confidence that a peer has to ensure that it will be treated fairly and securely, when interacting with another peer, for example, during transactions or downloading files,* especially by preventing malicious operations and collusion schemes (Zhu, Jajodia, & Kankanhalli, 2006). To address this issue, Bitcoin has brought two fundamental innovations, which, together, provide for the *self-governability* and *self-sustainability* of the network. The first innovation is the *blockchain*, which relies on public-private key encryption and hashing algorithms to create a decentralised, append-only and tamper-proof database. The second innovation is *Proof-of-Work*, a decentralised consensus protocol using cryptography and economic incentives to encourage people to operate and simultaneously secure the network. Accordingly, the Bitcoin protocol represents an elegant, but purely technical solution to the issue of social trust – which is normally resolved by relying on trusted authorities and centralised intermediaries. With the blockchain, to the extent that trust is delegated to the technology, individuals who do not know (and therefore do not necessarily trust) each other, can now transact with one another on a peer-to-peer basis, without the need for any intermediary.

Hence Bitcoin uses cryptography not as a way to preserve the secrecy of transactions, but rather in order to create a *trustless infrastructure* for financial transactions. In this context, cryptography is merely used as a discrete notational system (DuPont, 2014) designed to promote the autonomy of the system, which can operate independently of any centralised third party [5]. It relies on simple cryptographic primitives or building blocks (SHA256 hash functions and public-key cryptography) to resolve, in a decentralised manner, the double-spending problem [6] found in many virtual currencies. The scheme used by Bitcoin (*Proof-of-Work*) relies on a peer-to-peer network of validators (or *miners*) who commit their computational resources (*hashing power*) to the network in order to record all valid transactions into a decentralised public ledger (a.k.a. the *blockchain*) in a chronological order. All valid transactions are recorded into a block, which incorporates a reference (or *hash*) to the previous block – so that any attempt at tampering with the order or the content of any past transaction will always and necessarily result in an apparent discontinuity in the chain of blocks.

By combining a variety of existing technologies with basic cryptographic primitives, Bitcoin has created a system that is provably secure, practically incorruptible and probabilistically unattackable [7] – all this, without resorting to any centralised authority in charge of policing the network. Bitcoin relies on a fully open and decentralised network, designed in such a way that anyone is free to use the network and contribute to it, without the need for any kind of previous identification. Yet, contrary to popular belief, Bitcoin is neither anonymous nor privacy-friendly. Quite the contrary, anyone with a copy of the blockchain can see the history of all Bitcoin transactions. Decentralised verification requires, indeed, that every transaction be made available for validation to all nodes in the network and that every transaction ever done on the Bitcoin network can be traced back to its origin. [8]

In sum, Bitcoin embodies in its very protocols a profoundly market-driven approach to social coordination, premised on strong assumptions of rational choice (Olson, 1965) and game-theoretical principles of non-cooperation (von Neumann & Morgenstern, 1953 [1944]). The (self-)regulation of the overall system is primarily achieved through a system relying on *perfect information* (the blockchain), combined with a consensus protocol and incentives mechanism (Proof-of-work), to govern the mutually adjusting interests of all involved actors. Other dimensions of social trust and coordination (such as loyalty, coercion, etc.) are seemingly

expunged from a system which expressly conforms to Hayek's ideals of *catallactic* organisation (Hayek, 1976, p. 107ff).

B. FROM INCEPTION TO CRISIS

1. A short history of Bitcoin

The history of Bitcoin – albeit very short – consists of a very intense series of events, which have led to the decentralised cryptocurrency becoming one of the most widely used forms of digital cash. The story began in October 2008, with the release of the Bitcoin white paper (Nakamoto, 2008a). In January 2009, the Bitcoin software was published and the first block of the Bitcoin blockchain was created (the so-called *Genesis block*) with a release of 50 bitcoins. Shortly after, the first Bitcoin transaction took place between Satoshi Nakamoto and Hal Finney – a well-known cryptographer and prominent figure of the cypherpunk movement in the 1990s. It is not until a few months later that Bitcoin finally acquired an equivalent value in fiat currency [9] and slowly made its way into the commercial realm, as it started being accepted by a small number of merchants. [10]

In the early days, Satoshi Nakamoto was actively contributing to the source code and collaborating with many of the early adopters. Yet, he was always very careful to never disclose any personal details, so as to maintain his identity secret. To date, in spite of the various theories that have been put forward, [11] the real identity of Satoshi Nakamoto remains unknown. In a way, the pseudonymity of Satoshi Nakamoto perfectly mirrors that of his brainchild, Bitcoin – a technology designed to substitute technology for trust, thus rendering the identification of transacting parties unnecessary.

Over the next few months, Bitcoin adoption continued to grow, slowly but steadily. Yet, the real spike in popularity of Bitcoin was not due to increased adoption by commercial actors, but rather to the establishment in January 2011 of *Silk Road* – an online marketplace (mostly used for the trading of illicit drugs) relying on Tor and Bitcoin to preserve the anonymity of buyers and sellers. Silk Road paved the way for Bitcoin to enter the mainstream, but also led many governmental agencies to raise several concerns that Bitcoin could be used to create black markets, evade taxation, facilitate money laundering and even support the financing of terrorist activities.

In April 2011, to the surprise of many, Satoshi Nakamoto announced on a public mailing list that he would no longer work on Bitcoin. *I've moved on to other things* he said, before disappearing without further justification. Yet, before doing so, he transferred control over the source code repository of the Bitcoin client to Gavin Andresen, one of the main contributors to the Bitcoin code. Andresen, however, did not want to become the sole leader of such a project, and thus granted control over the code to four other developers – Pieter Wuille, Wladimir van der Laan, Gregory Maxwell, and Jeff Garzik. Those entrusted with these administration rights for the development of the Bitcoin project became known as the *core developers*.

As the popularity of Bitcoin continued to grow, so did the commercial opportunities and regulatory concerns. However, with the exit of Satoshi Nakamoto, Bitcoin was left without any leading figure or institution that could speak on its behalf. This is what justified the creation, in September 2012, of the Bitcoin Foundation – an American lobbying group focused on standardising, protecting and promoting Bitcoin. With a board comprising some of the biggest names in the Bitcoin space (including Gavin Andresen himself), the Bitcoin Foundation was intended to do for Bitcoin what the Linux Foundation had done for open source software: paying developers to work full-time on the project, establishing best practices and, most importantly, bringing legitimacy and building trust in the Bitcoin ecosystem. And yet, concerns

were raised regarding the legitimacy of this self-selected group of individuals – many of whom had dubious connections or were allegedly related to specific Bitcoin scams [12] – to act as the referent and public face of Bitcoin. Beyond the irony of having a decentralised virtual currency like Bitcoin being represented by a centralised profit-driven organisation, it soon became clear that the Bitcoin Foundation was actually unable to take on that role. Plagued by a series of financial and management issues, with some of its ex-board members under criminal investigation and most of its funds depleted, the Bitcoin Foundation has today lost much of its credibility.

But even the fall of the Bitcoin Foundation did not seem to significantly affect Bitcoin – probably because the Foundation was merely a *facade* that never had the ability to effectively control the virtual currency. Bitcoin adoption has continued to grow over the past few years, to eventually reach a market capitalisation of almost US 7 billion dollars. Bitcoin still has no public face and no actual institution that can represent it. Yet, people continue to use it, to maintain its protocol, and to rely on its technical infrastructure for an increasing number of commercial (and non-commercial) operations. And although a few Bitcoin-specific regulations have been enacted thus far (see e.g. the NY State BitLicense), regulators around the world have, for the most part, refrained from regulating Bitcoin in a way that would significantly impinge upon it (De Filippi, 2014).

Bitcoin thus continues to operate, and continues to be regarded (by many) as an open source software platform that relies on a decentralised peer-to-peer network governed by distributed consensus. Yet, if one looks at the underlying reasons why Bitcoin has been created in the first place, and the ways it has eventually been adopted by different categories of people, it becomes clear that the original conception of Bitcoin as a decentralised platform for financial disruption has progressively been compromised by the social and cultural context in which the technology operates.

Following the first wave of adoption by the cypherpunk community, computer geeks and crypto-libertarians, a second (larger) wave of adoption followed the advent of Silk Road in 2011. But what actually brought Bitcoin to the mainstream were the new opportunities for speculation that emerged around the cryptocurrency, as investors from all over the world started to accumulate bitcoins (either by purchasing them or by mining) with the sole purpose of generating profits through speculation. This trend is a clear reflection of the established social, economic and political order of a society driven by the capitalistic values of accumulation and profit maximisation. Accordingly, even a decentralised technology specifically designed to promote disintermediation and financial disruption can be unable to protect itself from the inherent tendencies of modern capitalist society to concentrate wealth and centralise power into the hands of a few (Kostakis & Bauwens, 2014).

The illusion of Bitcoin as a decentralised global network had already been challenged in the past, with the advent of large mining pools, mostly from China, which nowadays control over 75% of the network. But this is only one part of the problem. It took a simple – yet highly controversial – protocol issue to realise that, in spite of the open source nature of the Bitcoin platform, the governance of the platform itself is also highly centralised.

2. The block size dispute

To many outside observers, the contentious issue may seem surprisingly specific. As described earlier, the blockchain underpinning the Bitcoin network is composed of a series of blocks listing the totality of transactions which have been executed so far. For a number of reasons (mainly related to preserving the security and stability of the system, as well as to ensure easy

adoption), the size of these blocks was initially set at 1 megabyte. In practice, however, this technical specification also sets a restriction on the number of transactions which the blockchain can handle in a particular time frame. Hence, as the adoption of Bitcoin grew, along with the number of transactions to be processed, this arbitrary limitation (which was originally perceived as being innocuous) became the source of heated discussions – on several internet forums, blogs, and conferences – leading to an important dispute within the Bitcoin community (Rizzo, 2016). Some argued that the one megabyte cap was effectively preventing Bitcoin from scaling and was thus a crucial impediment to its growth. Others claimed that many workarounds could be found (e.g. off-chain solutions that would take off the load from the main Bitcoin blockchain) to resolve this problem without increasing the block size. They insisted that maintaining the cap was necessary both for security reasons and for *ideological* reasons, and was a precondition to keeping the system more inclusive and decentralised.

On 15 August 2015, failing to reach any form of consensus over the issue of block sizes, a spinoff project was proposed. Frustrated by the reluctance expressed by the other Bitcoin developers to officially raise the block size limit (Hearn, 2015), two core developers, Gavin Andresen and Mike Hearn, released a new version of the Bitcoin client software (Bitcoin XT) with the latent capacity of accepting and producing an increased block size of eight megabytes. This client constitutes a particular kind of *fork* of the original software or reference client (called Bitcoin Core). Bitcoin XT was released as a soft fork, [13] with the possibility to turn into a hard fork, if and when a particular set of conditions were met. Initially, the software would remain identical to the Bitcoin Core software, with the exception that all the blocks mined with the Bitcoin XT software would be "signed" by XT. This signature serves as a proxy for a poll: starting from 11 January 2016, in the event that at least 75% of all most recent 1,000 blocks have been signed by XT, the software would start accepting and producing blocks with a maximum block size of eight megabytes – with the cap increasing linearly so as to double every two years. This would mark the beginning of an actual *hard fork*, leading to the emergence of two blockchain networks featuring two different and incompatible protocols.

The launch of Bitcoin XT proved highly controversial. It generated a considerable amount of debate among the core developers, and eventually led to a full-blown conflict which has been described as a *civil war* within the Bitcoin community (Hearn, 2016). Among the Bitcoin core developers, Gregory Maxwell in particular was a strong proponent of maintaining the 1 megabyte cap. According to him, increasing the block size cap would constitute a risky change to the fundamental rules of the system, and would inherently bring Bitcoin towards more centralisation – because it would mean that less powerful machines (such as home computers) could no longer continue to handle the blockchain, thus making the system more prone to being overrun by a small number of big computers and mining pools. Similarly, Nick Szabo – a prominent cryptographer involved since the early days in the cypherpunk community – declared that increasing the block size so rapidly would constitute a huge security risk that could jeopardise the whole network. Finally, another argument raised against the Bitcoin XT proposal was that increasing the block size would possibly lead to variable, and delayed confirmation times (as larger blocks may fail to be confirmed every ten minutes).

Within the broader Bitcoin community, the conflict gave rise to copious amounts of flame-wars in various online forums that represent the main sources of information for the Bitcoin community (Reddit, Bitcoin Info, Bitcoin.org, etc.). Many accused the proponents of Bitcoin XT of using populist arguments and alarmist strategies to bring people on their side. Others claimed that, by promoting a hard fork, Bitcoin XT developers were doing exactly what the Bitcoin protocol was meant to prevent: they were creating a situation whereby people from each side of

the network would be able to spend the same bitcoins twice. In some cases, the conflict eventually resulted in outright censorship and banning of Bitcoin XT supporters from the most popular Bitcoin websites. [14] Most critically, the conflict also led to a variety of personal attacks towards Bitcoin XT proponents, and several online operators who expressed support for Bitcoin XT experienced Distributed Denial of Service (DDoS) attacks.

In the face of these events, and given the low rate of adoption of Bitcoin XT by the Bitcoin community at large, [15] Mike Hearn, one of the core developers and key instigators of Bitcoin XT, decided to resign from the development of Bitcoin – which he believed was on the brink of technical collapse. Hearn condemned the emotionally charged reactions to the block size debate, and pointed at major disagreements among the appointed Bitcoin core developers in the interpretation of Nakamoto's legacy.

But the conflict did not end there. Bitcoin XT was only the first of a series of improvements which were subsequently proposed to the Bitcoin protocol. As Bitcoin XT failed to gain mass adoption, it was eventually abandoned on January 23rd. New suggestions were made to resolve the block size problem (see e.g., Bitcoin Unlimited, Bitcoin Classic, BitPay Core). The most popular today is probably Bitcoin Classic, which proposes to increase the block size cap to 2 megabytes (instead of 8) by following the same scheme as Bitcoin XT (i.e. after 75% of bitcoin miners will have endorsed the new format). One interesting aspect of Bitcoin Classic is that it also plans to set up a specific governance structure that is intended to promote more democratic decision-making with regard to code changes, by means of a voting process that will account for the opinions of the broader community of miners, users, and developers. Bitcoin Classic has received support from relevant players in the Bitcoin community, including Gavin Andresen himself, and currently accounts for 25% of the Bitcoin network's nodes.

It is, at this moment in time, quite difficult to predict where Bitcoin is heading. Some may think that the Bitcoin experiment has failed and that it is not going anywhere; [16] others may think that Bitcoin will continue to grow in underserved and inaccessible markets as a gross settlement network for payment obligations and safe haven assets; [17] while many others believe that Bitcoin is still heading *to the moon* and that it will continue to surprise us as time goes on. [18] One thing is sure though: regardless of the robustness and technical viability of the Bitcoin protocol, this governance crisis and failure in conflict resolution has highlighted the fragility of the current decision-making mechanisms within the Bitcoin project. It has also emphasised the tension between the (theoretically) decentralised nature of the Bitcoin network and the highly centralised governance model that has emerged around it, which ultimately relied on the goodwill and aligned interests of only a handful of people.

II. BITCOIN GOVERNANCE AND ITS CHALLENGES

Governance structures are set up in order to adequately pursue collective goals, maintain social order, channel interests and keep power relations under check, while ensuring the *legitimacy* of actions taken collectively. They are therefore closely related to the issue of *trust*, which is a key aspect of social coordination and which online socio-technical systems address by combining informal interpersonal relations, formal rules and technical solutions in different ways (Kelty, 2005). In the case of online peer-production communities, two essential features are decisive in shaping their governance structure, namely the fact that they are *volunteer-driven* and that they seek to *self-organise* (Benkler, 2006). Thus, compared to more traditional forms of organisations such as firms and corporations, they often need to implement alternative means of

coordination and incentivisation (Demil & Lecocq, 2006).

Nicolas Auray has shown that, although the nature of online peer-production communities can be very different (ranging from *Slashdot* to *Wikipedia* and *Debian*), they all face three key challenges which they need to address in order to thrive (Auray, 2012):

- definition and protection of *community borders*;
- establishment of *incentives* for participation and acknowledgment of the *status* of contributors;
- and, finally, pacification of *conflicts*.

Understanding how each of these challenges is addressed in the case of the Bitcoin project is particularly difficult, since Bitcoin is composed of two separate, but highly interdependent layers, which involve very different coordination mechanisms. On the one hand, there is the *infrastructural* layer: a decentralised payment system based on a global *trustless* peer-to-peer network which operates according to a specific set of protocols. On the other hand, there is the layer of the *architects*: a small group of developers and software engineers who have been *entrusted* with key roles for the development of this technology.

The Bitcoin project can thus be said to comprise at least two different types of communities – each with their own boundaries and protection mechanisms, rewards or incentive systems, and mechanisms for conflict resolution. One is the community of nodes within the network, which includes both *passive* users merely using the network to transfer money around, and "active" users (or miners) contributing their own computational resources to the networks in order to support its operations. The other is the community of developers, who are contributing code to the Bitcoin project with a view to maintain or improve its functionalities. What the crisis described above has revealed is the difficulty of establishing a governance structure which would properly interface both of these dimensions. As a consequence, a small number of individuals became responsible for the long-term sustainability of a large collective open source project, and the project rapidly fell prone to interpersonal conflict once consensus could no longer be reached among them.

This section will describe the specificities of the two-layered structure of the Bitcoin project and the mechanisms put in place to address these key challenges, in order to better understand any shortcomings they may display.

A. THE BITCOIN NETWORK: GOVERNANCE BY INFRASTRUCTURE

As described earlier, the Bitcoin network purports to be both *self-governing* and *self-sustaining*. [19] As a trustless infrastructure, it seeks to function independently of any social institutions. The rules governing the platform are not enforced by any single entity, instead they are embedded directly into the network protocol that every user must abide to. [20]

Given the open and decentralised nature of the Bitcoin network, its *community borders* are extremely flexible and dynamic, in that everyone is free to participate and contribute to the network – either as a passive user or as an active miner. The decentralised character of the network however, creates significant challenges when it comes to the protection thereof, mainly due to the lack of a centralised authority in charge of policing it. Bitcoin thus implemented a technical solution to protect the network against malicious attacks (e.g. so-called *sybil attacks*) through the Proof-of-Work mechanism, designed to make it economically expensive to cheat the network. Yet, while the protocol has proved successful thus far, it remains subject to a lot of criticism. Beyond the problems related to the high computational costs of Proof-of-Work, [21] the

Bitcoin network can also be co-opted by capital. If one or more colluding actors were to control at least 51% of the network's hashing power, they would be able to arbitrarily censor transactions by validating certain blocks at the expense of others (the so-called 51% attack).

With regard to *status recognition*, the Bitcoin protocol eliminates the problem at the root by creating a trustless infrastructure where the identity of the participant nodes is entirely irrelevant. In Bitcoin, there is no centralised authority in charge of assigning a network identifier (or account) to each individual node. The notions of identity and status are thus eradicated from the system and the only thing that matters – ultimately – is the amount of computational resources that every node is providing to the network.

Conversely, the reward system represents one of the constitutive elements of the Bitcoin network. The challenge has been resolved in a purely technical manner by the Bitcoin protocol, through the notion of *mining*. In addition to providing a protection mechanism, the Proof-of-Work algorithm introduces a series of economic incentives to reward those who are contributing to maintaining and securing the network with their computational resources (or *hashing power*). The mining algorithm is such that the first one to find the solution to a hard mathematical problem (whose difficulty increases over time) [22] will be able to register a new block into the blockchain and will earn a specific amount of bitcoins as a reward (the reward was initially set at 50 bitcoins and is designed to be halved every four years). From a game-theoretical perspective, this creates an interesting incentive for all network participants to provide more and more resources to the network, so as to increase their chances of being rewarded bitcoins. [23] Bitcoin's incentive mechanism is thus a complicated, albeit mathematically elegant way of bringing a decentralised network of self-interested actors to collaborate and contribute to the operations of the Bitcoin network by relying exclusively on mathematical algorithms and cryptography. Over time, however, the growing difficulty of mining due to the increasing amount of computational resources engaged in the network, combined with the decreasing amount of rewards awarded by the network, has eventually led to a progressive concentration of hashing power into a few *mining pools, *which are today controlling a large majority of the Bitcoin network – thereby making it more vulnerable to a 51% attack. [24] Hence, in spite of its original design as a fully decentralised network ruled by distributed consensus, in practice, the Bitcoin network has evolved into a highly centralised network ruled by an increasingly oligopolistic market structure.

Finally, with regard to the issue of *conflict resolution*, it is first important to determine what constitutes a conflict at the level of the Bitcoin infrastructure. If the purpose of the Bitcoin protocol is for a decentralised network of peers to reach consensus as to what is the right set of transactions (or *block*) that should be recorded into the Bitcoin blockchain, then a conflict arises whenever two alternative blocks (which are both valid from a purely mathematical standpoint) are registered by different network participants in the same blockchain – thus creating two competing versions (or *forks*) of the same blockchain. Given that there is no way of deciding *objectively* which blockchain should be favoured over the other, the Bitcoin protocol implements a specific fork-choice strategy stipulating that, if there is a conflict somewhere on the network, the longest chain shall win. [25] Again, as with the former two mechanisms, the longest-chain rule is a simple and straightforward mechanism to resolve the emergence of conflicts within the Bitcoin network by relying – solely and exclusively – on technological means.

It is clear from this description, that the objective of Satoshi Nakamoto and the early Bitcoin developers was to create a decentralised payment system that is both self-sufficient and self-

contained. Perhaps naively, they thought it was possible to create a new technological infrastructure that would be able to govern itself – through its own protocols and rules – and that would not require any third-party intervention in order to sustain itself. And yet, in spite of the mathematical elegance of the overall system, once introduced in a particular socio-economic context, technological systems often evolve in unforeseen ways and may fall prey to unexpected power relations.

In the short history of Bitcoin, indeed, there have been significant tensions related to *border protection*, *rewards systems* and *conflict resolution*. Some of these issues are inherent in the technological infrastructure and design of the Bitcoin protocol. Perhaps one of the most revealing of the possible ways of subverting the system is the notion of *selfish mining* whereby miners can increase their potential returns by refusing to cooperate with the rest of the network. [26] While this does not constitute a technical threat to the Bitcoin protocol *per se*, it can nonetheless be regarded as an *economic attack*, which contributes to potentially reducing the security of the Bitcoin network by changing the inherent incentive structure. [27] Other issues emerged as a result of more exogenous factors, such as the Mt. Gox scandal [28] of 2014 – which led to the loss of 774,000 bitcoins (worth more than US 450 million dollars at the time) – as well as many other scams and thefts that occurred on the Bitcoin network over the years. [29] Most of these were not due to an actual flaw in the Bitcoin protocol, but were mostly the result of ill-intentioned individuals and bad security measures in centralised platforms built on top of the Bitcoin network (Trautman, 2014).

Accordingly, it might be worth considering whether – independently of the technical soundness of the Bitcoin protocol – the Bitcoin network can actually do away with any form of external regulation and/or sanctioning bodies, or whether, in order to ensure the proper integration (and assimilation) of such a technological artefact within the social, economic and cultural contexts of modern societies, the Bitcoin network might require some form of surveillance and arbitration mechanisms (either internal or external to the system) in order to preserve legitimate market dynamics, as well as to guarantee a proper level of consumer protection and financial stability in the system.

B. THE BITCOIN ARCHITECTS: GOVERNANCE OF INFRASTRUCTURE

Just like many other internet protocols, Bitcoin was initially released as an open source software, encouraging people to review the code and spontaneously contribute to it. Despite their formal emphasis on *openness*, different open source software projects and communities feature very different social and organisational structures. The analysis of communication patterns among various open source projects has shown tendencies ranging from highly distributed exchanges between core developers and active users, to high degrees of centralisation around a single developer (Crowston & Howison, 2005). Moreover, different open source communities enjoy a more or less formalised governance structure, which often evolves as the project matures. Broadly speaking, open source communities have been categorised into two main types or configurations: *democratic-organic* versus "autocratic-mechanistic" (de Laat, 2007). The former display a highly structured and meritocratic governance system (such as the Debian community, most notably), whereas the latter feature less sophisticated and more

implicit governance systems, such as the Linux community, where most of the decision-making power has remained in the hands of Linus Torvald – often referred to as the "benevolent dictator'. Bitcoin definitely falls into the second category.

Indeed, since its inception, Satoshi Nakamoto was the main person in charge of managing the project, as well as the only person with the right to commit code into the official Bitcoin repository. It was only at a later stage, when Satoshi began to disengage from the Bitcoin project, that this power was eventually transferred to a small group of 'core developers'. Hence, just like many other open source projects, there is a discrepancy between those who can provide input to the project (the community at large) and those who have the ultimate call as to where the project is going. Indeed, while anyone is entitled to submit changes to the software (such as bug fixes, incremental improvements, etc.), only a small number of individuals (the core developers) have the power to decide which changes shall be incorporated into the main branch of the software. This is justified partly by the high level of technical expertise needed to properly assess the proposed changes, but also – more implicitly – by the fact that the core developers have been entrusted with the responsibility of looking after the project, on the grounds of their involvement (and, to some extent, shared *ideology*) with the original concept of Satoshi Nakamoto.

With this in mind, we can now provide a second perspective on the three key challenges facing Bitcoin, and analyse how they are being dealt with from the side of its *architects*: the Bitcoin developers.

The *definition and protection of community boundaries*, and of the work produced collectively, is a key issue in open source collectives. It classically finds a solution through the setting up of an alternative intellectual property regime and licensing scheme – *copyleft*, which ensures that the work will be preserved as a common pool resource – but also enforces a number of organisational features and rules intended to preserve some control over the project (O'Mahony, 2003; Schweik & English, 2007). In the case of Bitcoin, community borders are – at least in theory – quite clearly defined. Just like many other open source software projects, there exists a dividing line between the community of users and developers at large, who can provide input and suggest modifications to the code (by making a pull-request, for instance), and the core developers who are in charge of preserving the quality and the functionality of the code, and who are the only ones with the power to accept (or refuse) the proposed modifications (e.g. by merging pull-requests into the main branch of the code). However, the distinction between these two communities is not as clear-cut as it may seem, since the community at large also has an important (albeit indirect) influence on the decisions concerning the code.

Specifically, consensus formation among the Bitcoin core developers has been formalised through a process known as Bitcoin Improvement Proposals (BIPs) [30], which builds heavily on the process in place for managing the Python programming language (PEPs or Python Enhancement Proposals). Historically, both of these processes share similarities with (and sometimes explicitly refer to) what can be considered the "canonical" approach to consensus formation for designing and documenting network protocols: RFC or Request For Comments, used to create and develop the internet protocol suite (Flichy, 2007, p. 35ff). The BIP process requires that all source code and documentation be released and made available to anyone, so that a multiplicity of individuals can contribute to discuss and improve them. Yet, the final call as to whether a change will be implemented ultimately relies on the core developers assessing the degree of public support which a proposal has built, and finding a consensus among themselves:

> We are fairly liberal with approving BIPs, and try not to be too involved in decision making on behalf of the community. The exception is in very rare cases of dispute resolution when a decision is contentious and cannot be agreed upon. In those cases, the conservative option will always be preferred. Having a BIP here does not make it a formally accepted standard until its status becomes Active. For a BIP to become Active requires the mutual consent of the community. Those proposing changes should consider that ultimately consent may rest with the consensus of the Bitcoin users. [31]

This description provides a concise overview of the structures of legitimacy and accountability which govern the relationship between the Bitcoin architects (or core developers) and the Bitcoin users. While the community is open for anyone to participate, decision-making is delegated to a small number of people who try to keep intervention to a minimum. Yet, ultimately, the sovereignty of the overall project rests with *the people* – i.e. the Bitcoin users and miners. If the core developers were to make a modification to the code that the community disagrees with (the miners, in particular), the community might simply refuse to run the new code. This can be regarded as a form of "vetoing power' [32] or "market-based governance' [33] which guarantees that legitimacy of the code ultimately rests with the users.

Regarding *acknowledgment of status*, this requires balancing rewards for the most active and competent contributors, while promoting and maintaining the collective character of the overall endeavour. Indeed, open source developers are acutely aware of the symbolic retributions which they can acquire by taking part in a given project, and are also monitoring other contributors to assess their position within communities which display a strongly meritocratic orientation (Stewart, 2005). Some communities rank individuals by resorting to systems of marks which provide a quantitative metric for reputation; others rely on much less formalised forms of evaluation. In the case of Bitcoin, some measure of reputation can be derived from the platform used to manage the versioning of the software – *Github* – which includes metrics for users" activities (such as number of contributions, number of followers, etc.). However, the reputation of the core developers is on a completely different scale, and is mostly derived from their actual merit or technical expertise, as well as a series of less easily defined individual qualities which can be understood as a form of *charisma*.

Finally, *conflict management* is probably the most difficult issue to deal with in consensus-oriented communities, since it requires a way to avoid both *paralysing deadlocks* and *divisive fights*. Taking Wikipedia as an example, the community relies on specific mechanisms of mutual surveillance as the most basic way of managing conflicts; however, additional regulatory procedures of mediation and sanctions have been established and can be resorted to if needed (Auray, 2012, p. 225). The Debian community is also well known for its sophisticated rules and procedures (Lazaro, 2008). Though not immune to deadlocks and fighting, these communities have managed to scale while maintaining some degree of inclusivity, by shifting contentious issues from *substantive* to *procedural* grounds – thus limiting the opportunities for personal disputes and *ad hominem* attacks.

Obviously, the Bitcoin community lacks any such form of conflict management procedures. As described above, failure to reach consensus among the core developers concerning the block size dispute led to an actual forking of the Bitcoin project. Forking is a process whereby two (or more) software alternatives are provided to the user base, who will therefore need to make a choice: the adoption rate will ultimately determine which branch of the project will win the

competition, or whether they will both evolve as two separate branches of the same software. Forking is standard practice in free/*libre* and open source software development, and although it can be seen as a last resort solution which can sometimes put the survival of a project at risk (Robles & González-Barahona, 2012), it can also be considered a key feature of its governance mechanisms. For Nyman and Lindman: *The right to fork code is built into the very definition of what it means to be an open source program* – it is a reminder that developers have the essential freedom to take the code wherever they want, and this freedom also functions as a looming threat of division that binds the developer community together (Nyman & Lindman, 2013).

In sum, it can be stressed that, at all three levels (defining borders, acknowledging status, and managing conflicts), the governance of the Bitcoin project relies almost exclusively on its leaders, lending credit to the view that peer production can often lead to the formation of oligarchic organisational forms (Shaw & Hill, 2014). More specifically, in classic weberian terms – and as can often be observed in online communities – Bitcoin governance consists in a form of domination based on charismatic authority (O'Neil, 2014), largely founded on presumed technical expertise. The recent crisis experienced by the Bitcoin community revealed the limits of consensus formation between individuals driven by sometimes diverging political and commercial interests, and underlined the discrepancies between the overall goals of the project (a self-regulating decentralised virtual currency and payment system) and the excessively centralised and technocratic elites who are in charge of the project.

III. THE INVISIBLE POLITICS OF BITCOIN

Vires in Numeris (latin for: *Strength in Numbers*) was the motto printed on the first physical Bitcoin wallets [34] – perhaps as an ironic reference to the "*In God we Trust"* motto printed on US dollar bills. In the early days, the political objectives of Bitcoin were clearly and explicitly stated through the desire of changing existing power dynamics between individuals and the state. [35] Yet, while some people use Bitcoin as a vehicle for expressing their political views (e.g. the community of so-called cypherpunks and *crypto-libertarians*), others believe that there is no real political ideology expressed within the technology itself. [17] Indeed, if asked, many will say that one of the core benefits of Bitcoin is that it operates beyond the scope of governments, politics, and central banks. [36] But it does not take much of a stretch to realise that this desire to remain *a-political* constitutes a political dimension in and of itself (Kostakis & Giotitsas, 2014).

Decentralisation inherently affects political structures by removing a control point. Regarding Bitcoin, decentralisation is achieved through a peer-to-peer payment system that operates independently of any (trusted) third party. As a result, not only does Bitcoin question one of the main prerogatives of the state – that of money issuance and regulation, it also sheds doubts on the need (and, therefore, the legitimacy) of existing financial institutions. On the one hand, as a decentralised platform for financial transactions, Bitcoin sets a limit on the power of central banks and other financial institutions to define the terms and conditions, and control the execution of financial transactions. On the other hand, by enabling greater disintermediation, the Bitcoin blockchain provides new ways for people to coordinate themselves without relying on a centralised third party or trusted authority, thus potentially promoting individual freedoms and emancipation. [37] More generally, the blockchain is now raising high hopes as a solution which, beyond a payments system, could support many forms of direct interactions between free and equal individuals – with the implicit assumption that this would contribute to furthering democratic goals by promoting a more horizontal and self-organising social structure

(Clippinger & Bollier, 2014).

As Bitcoin evolves – and in the eventuality that it gets more broadly adopted – it will need to face a growing number of technical challenges (e.g. related to blockchain scalability), but it will also encounter a variety of social and political challenges – as the technology will continue to impinge upon existing social and governmental institutions, ushering in an increasingly divergent mix of political positions.

The mistake of the Bitcoin community was to believe that, once technical governance had been worked out, the need to rely on government institutions and centralised organisations in order to manage and regulate social interactions would eventually disappear (Atzori, 2015; Scott, 2014). Politics would progressively give way to new forms of technologically-driven protocols for social coordination (Abramowicz, 2015) – regarded as a more efficient way for individuals to cooperate towards the achievement of a collective goal while preserving their individual autonomy.

Yet, one cannot get rid of politics through technology alone, because the governance of a technology is – itself – inherently tied to a wide range of power dynamics. As Yochai Benkler elegantly puts it, there are no *spaces of perfect freedom from all constraints,* only different sets of constraints that one necessarily must choose from (Benkler, 2006). Bitcoin as a trustless technology might perhaps escape the existing political framework of governmental and market institutions; yet, it remains subject to the (invisible) politics of a handful of individuals – the programmers who are in charge of developing the technology and, to a large extent, deciding upon its functionalities.

Implicit in the governance structure of Bitcoin is the idea that the Bitcoin core developers (together with a small number of technical experts) are – by virtue of their technical expertise – the most likely to come up with the right decision as to the specific set of technical features that should be implemented in the platform. Such a *technocratic* approach to governance is problematic in that it goes counter to the original conception of the Bitcoin project. There exists, therefore, an obvious discrepancy between the libertarian vision of Bitcoin as a decentralised infrastructure that cannot be regulated by any third party institution, and the actual governance structure that dictates the technological development of Bitcoin – which, in spite of its open source nature, is highly centralised and undemocratic. While the (a)political dimension of the former has been praised or at least acknowledged by many, the latter has remained, for a long time, invisible to the public: the technical decisions to be taken by the Bitcoin developers were not presented as political decisions, and were therefore never debated as such.

The block size debate is a good illustration of this tendency. Although the debate was framed as a value-neutral technical discussion, most of the arguments in favour or against increasing the size of a block were, in fact, part of a hidden political debate. Indeed, except for the few arguments concerning the need to preserve the security of the system, most of the arguments that animated the discussion were, ultimately, concerned with the socio-political implications of such a technical choice (e.g. supporting a larger amount of financial transactions versus preserving the decentralised nature of the network). Yet, insofar as the problem was presented as if it involved only rational and technical choices, the political dimensions which these choices might involve were not publicly acknowledged.

Moreover, if one agrees that *all artefacts have politics* (Winner, 1980) and that technology frames social practice (Kallinikos, 2011), it follows that the design and features of the Bitcoin platform must be carefully thought through by taking into account not only its impact on the

technology as such (i.e. security and scalability concerns), but also its social and political implications on society at large.

Politics exist because, in many cases, consensus is hard to achieve, especially when issues pertaining to *social justice *need to be addressed. Social organisations are thus faced with the difficult challenge of accommodating incompatible and often irreconcilable interests and values. The solutions found by modern day liberal democracies involve strong elements of *publicity* and *debate*. The underlying assumption is that the only way to ensure the *legitimacy* of collective decisions is by making conflicts apparent and by discussing and challenging ideas within the public sphere (Habermas, 1989). Public deliberations and argumentation are also necessary to achieve a greater degree of *rationality* in collective decisions, as well as to ensure full *transparency* and *accountability* of the ways in which these decisions are both made and put into practice. But the antagonistic dimensions of social life constantly undermine the opportunities for consensus formation. A truly democratic approach needs, therefore, to acknowledge – and, ideally, to balance or compromise – these spaces of *irreconcilable dissent* which are the most revealing of embedded power relations (Mouffe & Laclau, 2001; Mouffe, 1993).

This is perhaps even more crucial for technologies such as the internet or Bitcoin, which seek to implement a global and shared infrastructure for new forms of coordination and exchange. Bitcoin as an *information infrastructure* must be understood here as a means of introducing and shaping a certain type of social relations (Star, 1999; Bowker et al., 2010). Yet, just like many other infrastructures, Bitcoin is mostly an *invisible* technology that operates in the background (Star & Strauss, 1999). It is, therefore, all the more important to make the design choices lying behind its technical features more visible, in order to shed light on the politics which are implicit in the technological design.

It should be clear, by now, that the political intentions of a technology cannot be resolved, only and exclusively, by technological means. While technology can be used to steer and mediate many kinds of social interactions, it should not (and cannot) be the sole and main driver of social change. As Bitcoin has shown, it is unrealistic to believe that human organisations can be governed by relying exclusively on algorithmic rules. In order to ensure the long-term sustainability of these organisations, it is necessary to incorporate, on top of the technical framework, a specific governance structure that enables people to discuss and coordinate themselves in an authentically democratic way, but also – and perhaps more importantly – to engage and come up with decisions as to how the technology should evolve. In that regard, one should always be wary that the decision-making process involve not only those who are building the technology (i.e. developers and software engineers) but also all those who will ultimately be affected by these decisions (i.e. the users of that technology).

Different dimensions of the internet have already been analysed from such a perspective within the broader framework of internet governance (DeNardis, 2012; Musiani et al., 2016), providing important insights about the performative dimensions of the underlying software and protocols, and the ways they have been put to use. These could prove useful in better understanding and formulating a novel governance structure for the Bitcoin project – one that is mediated (rather than dictated) by technological rules.

CONCLUSION: BITCOIN WITHIN THE WIDER FRAME OF INTERNET GOVERNANCE

The internet, understood as a complex and heterogeneous socio-technical construct, combines many different types of arrangements – involving social norms, legal rules and procedures, market practices and technological solutions – which, taken together, constitute its overall governance and power structures (Brousseau, Marzouki, & Méadel, 2012). Most of the research on internet governance has focused on the interplay between *infrastructures* on the one hand, and *superstructures* or institutions on the other – particularly those which have emerged on top of the network during the course of its history (such as ICANN or IETF), sometimes generating conflictual relationships with existing national and international legal frameworks, private corporations, or even civil society at large (Mueller, 2002; Mueller, 2010; Mathiason, 2009; DeNardis, 2009; Bygrave & Bing, 2009). [38]

Internet governance has been fraught with many frictions, controversies and disputes over the years – an international fight to control the basic rules and protocols of the internet described by some as a *global war* (DeNardis, 2014). Even the much praised governance model of the internet protocol suite – based on the IETF's (deceptively simple) rule of *"rough consensus and running code*" – effectively involved, at certain points, fair amounts of power struggles and even autocratic design (Russell, 2014). The idea that consensus over technical issues can be reached more easily because it only involves objective criteria and factual observations (i.e. something either works or doesn't) neglects the reality that "stories about standards are necessarily about power and control – they always either reify or change existing conditions and are always conscious attempts to shape the future in specific ways" (Russell, 2012).

Set within the wider frame and history of internet governance, the Bitcoin case is particularly instructive insofar as it draws on a certain number of new, but also already existing practices, to promote some of the ideals which have been associated with the internet since its inception: furthering individual autonomy and supporting collective self-organisation (Loveluck, 2015). As we have seen, Bitcoin can be understood as a dual-layered construct, composed of a global network infrastructure on the one hand, and a small community of developers on the other. Although the *trustlessness* of the network seeks to obliviate the need for a central control point, in practice, as soon as a technology is deployed, new issues emerge from unanticipated uses of technology – which ultimately require the setting up of social institutions in order to protect or regulate the technology. These institutions can be more or less attuned with the overall aims of the technology, and can steer it in different directions. For instance, while the IETF managed to implement a relatively decentralised and bottom-up process for establishing standards, the Domain Name System (DNS) has shown that even a distributed network might, at some point, need to rely on a centralised control point to administer *scarce resources* (such as domain names). This has led to the emergence of centralised – and somewhat contested – institutions, such as, most notably, the ICANN – a US-based non-profit corporation that is in charge of coordinating all unique identifiers across the world wide web.

The lessons from the past – taking account of both the success stories and failures of internet governance – can serve as useful indications as to what should be attempted or, on the contrary, avoided in terms of Bitcoin governance. In particular, it should be acknowledged that socio-technical systems cannot – by virtue of their embeddedness into a social and cultural context – ensure their own *self-governance* and *self-sustainability* through technology alone. Any technology will eventually fall prey to the social, cultural and political pressures of the context in

which it operates, which will very probably make it grow and evolve in unanticipated directions (Akrich, 1989; MacKenzie & Wajcman, 1999).

The Bitcoin project has evolved significantly over the years, for reasons which are both endogenous and exogenous to the system. From a small network run by a few crypto-libertarians and computer geeks eager to experiment with a new *liberation technology* (Diamond, 2010), the Bitcoin network quickly scaled into a global network which is struggling to meet the new demands and expectations of its growing user base and stakeholders.

The block size debate created an actual schism within the Bitcoin community – and, by doing so, ultimately stressed the need for a more democratic governance system. Drawing on the many different arrangements which have been experienced at different levels of internet governance, each with their own distinctive forms of deliberation and decision-making procedures (Badouard et al., 2012), the Bitcoin development process could perhaps be improved by introducing an alternative governance structure that would better account for the many other dimensions (other than technical) that the technology might have, especially with regard to its social, economic and political implications on society at large.

The Bitcoin Foundation was a first attempt in this direction, though it never managed to establish itself as a standardisation body precisely due to a lack of legitimacy and accountability in its own governance process. A centralised governance body (similar to ICANN) in charge of ensuring the legitimacy and accountability for the future developments of the Bitcoin project would obviously fail to obtain any kind of legitimacy from within the Bitcoin community – since eliminating the need for fiduciary institutions or other centralised authorities was the very purpose of the Bitcoin network. The technologically-driven approach currently endorsed by the Bitcoin project, aiming to create a governance structure that is solely and exclusively dictated by technological means (*governance by infrastructure*) has also been shown to be bound to failure, since a purely technological system cannot fully account for the whole spectrum (and complexity) of social interactions. In this regard, one of the main limitations of the Bitcoin protocol is that it is based on algorithmically quantifiable and verifiable actions (i.e. how much computing resources people are investing in the network) and it is therefore unable to reward those who contribute to the network in different manners, other than through hashing power.

A more interesting approach would involve using the underlying technology – the *blockchain* – not as a *regulatory technology* that will technologically enforce a particular set of predefined protocols and rules (as Bitcoin does), but rather as a platform on which people might encode their own sets of rules and procedures that will define a particular system of governance – one that can benefit from the distinctive characteristics of the blockchain (in terms of transparency, traceability, accountability, and incorruptibility) but would also leave room for the establishment of an institutional framework that could operate on top of that (decentralised) network. This would make sure that technology remains a tool of empowerment for people, who would use it to enable and support new models of governance, rather than the opposite.

Given the experimental nature and current lack of maturity of the technology, it is difficult to predict, at this specific point in time, what would be the best strategy to ensure that the Bitcoin project evolves in accordance with the interests of all relevant stakeholders. Yet, regardless of the approach taken, it is our belief that a proper governance structure for Bitcoin can only be achieved by publicly acknowledging its political dimensions, and replacing the current technocratic power structure of the Bitcoin project with an institutional framework capable of understanding (and accommodating) the politics inherent in each of its technical features.

REFERENCES

Abbate, J. (1999), *Inventing the Internet*, Cambridge, MA: MIT Press.

Abramowicz, M.B. (2015), *Peer-to-peer law, built on Bitcoin*, Legal Studies Research Paper, *GWU Law School,*http://scholarship.law.gwu.edu/faculty_publications/1109/

Agre, P.E. (2003), *P2P and the promise of Internet equality*, *Communications of the ACM 46*(2), pp. 39-42.

Akrich, M. (1989), *La construction d'un système socio-technique. Esquisse pour une anthropologie des techniques*, *Anthropologie et Sociétés 13*(2), pp. 31-54.

Atzori, M. (2015), *Blockchain technology and decentralized governance: is the State still necessary?*, working paper, *Available at SSRN*,
http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2709713

Auray, N. (2012), *Online communities and governance mechanisms*, in E. Brousseau, M. Marzouki & C. Méadel (eds.), *Governance, Regulation and Powers on the Internet*. Cambridge and New York: Cambridge University Press, pp. 211-231.

Badouard, R. et al (2012), *Towards a typology of Internet governance sociotechnical arrangements*, in F. Massit-Folléa, C. Méadel & L. Monnoyer-Smith (eds.), *Normative Experience in Internet Politics* Paris: Transvalor/Presses des Mines, pp. 99-124.

Benkler, Y. (2006), *The Wealth of Networks. How Social Production Transforms Markets and Freedom*. New Haven, CT: Yale University Press.

Benkler, Y. (2016), *Degrees of freedom, dimensions of power*, *Daedalus*145(1), pp. 18-32.

Bimber, B. (1994), *Three faces of technological determinism*, in M.R. Smith & L. Marx (eds.), *Does Technology Drive History? The Dilemma of Technological Determinism*. Cambridge, MA and London: MIT Press, pp. 79-100.

Bowker, G.C. et al (2010), *Toward Information Infrastructure Studies: ways of knowing in a networked environment*, in J. Hunsinger, L. Klastrup & M. Allen (eds.), *International Handbook of Internet Research*. Dordrecht and London: Springer, pp. 97-117.

Brousseau, E., Marzouki, M., & Méadel, C. eds. (2012), *Governance, Regulation and Powers on the Internet*. Cambridge and New York: Cambridge University Press.

Bygrave, L.A. & Bing, J. eds. (2009), *Internet Governance. Infrastructure and Institutions*. Oxford and New York: Oxford University Press.

Clippinger, J.H. & Bollier, D. eds. (2014), *From Bitcoin to Burning Man and Beyond. The Quest for Autonomy and Identity in a Digital Society, *Boston, MA and Amherst, MA: ID3 and Off the Common.

Crowston, K. & Howison, J. (2005), *The social structure of free and open source software development*, *First Monday [online] 10*(2),
http://firstmonday.org/ojs/index.php/fm/article/view/1207/1127

David, M. (2010), *Peer to Peer and the Music Industry. The Criminalization of Sharing*.

London, Thousand Oaks, CA, New Delhi and Singapore: Sage.

Demil, B. & Lecocq, X. (2006), *Neither market nor hierarchy nor network: the emergence of bazaar governance*, *Organization Studies 27*(10), pp. 1447-1466.

DeNardis, L. (2009), *Protocol Politics. The Globalization of Internet Governance*. Cambridge, MA: MIT Press.

DeNardis, L. (2012), *Hidden levers of Internet control. An infrastructure-based theory of Internet governance*, *Information, Communication & Society 15*(5), pp. 720-738.

DeNardis, L. (2014), *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Diamond, L. (2010), *Liberation technology*, *Journal of Democracy 21*(3), pp. 69-83.

Dingledine, R., Mathewson, N. & Syverson, P. (2004), *Tor: the second-generation onion router*, *Proceedings of the 13th USENIX Security Symposium*, San Diego, CA.

Dodd, N. (2014), *The Social Life of Money,* Princeton, NJ: Princeton University Press.

DuPont, Q. (2014), "The politics of cryptography: Bitcoin and the ordering machines", *Journal of Peer Production* (4), http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-politics-of-cryptography-bitcoin-and-the-ordering-machines/

Eyal, I. & Sirer, E.G. (2014), "Majority is not enough: Bitcoin mining is vulnerable", in *Financial Cryptography and Data Security,* Springer, pp. 436-454.

Ferguson, N. (2008), *The Ascent of Money. A Financial History of the World,* London: Penguin.

De Filippi, P. (2014), "Bitcoin: a regulatory nightmare to a libertarian dream", *Internet Policy Review 3*(2), http://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream

Flichy, P. (2007), *The Internet Imaginaire,* Cambridge, MA: MIT Press.

Gillespie, T. (2006), "Engineering a principle: 'end-to-end' in the design of the internet", *Social Studies of Science 36*(3), pp. 427-457.

Habermas, J. (1989), *The Structural Transformation of the Public Sphere. An Inquiry into a Category of Bourgeois Society,* Cambridge: Polity Press.

Hayek, F.A. (1976), *Law, Legislation and Liberty. Vol. 2, The Mirage of Social Justice*, London: Routledge & Kegan Paul.

Hayek, F.A. (1990), *The Denationalization of Money: The Argument Refined,* 3rd edition, London: The Institute of Economic Affairs.

Hearn, M. (2015), "Why is Bitcoin forking?", *Medium,* https://medium.com/faith-and-future/why-is-bitcoin-forking-d647312d22c1. Accessed 15 April 2016.

Hearn, M. (2016), "The resolution of the Bitcoin experiment", *Medium,*

https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7. Accessed 15 April 2016.

Hughes, E. (1993), "A Cypherpunk's Manifesto", http://www.activism.net/cypherpunk/manifesto.html. Accessed 24 March 2011.

Kahn, D. (1996), *The Codebreakers. The Story of Secret Writing,* 2nd edition, New York: Scribener.

Kallinikos, J. (2011), *Governing Through Technology. Information Artefacts and Social Practice,* Basingstoke and New York: Palgrave Macmillan.

Kelty, C. (2005), "Trust among the algorithms: ownership, identity, and the collaborative stewardship of information", in R.A. Ghosh (ed.), *Code. Collaborative Ownership and the Digital Economy,* Cambridge, MA: MIT Press, pp. 127-152.

Kostakis, V. & Bauwens, M. (2014), "Distributed capitalism", in *Network Society and Future Scenarios for a Collaborative Economy,* Basingstoke and New York: Palgrave Macmillan, pp. 30-34.

Kostakis, V. & Giotitsas, C. (2014), "The (a)political economy of bitcoin", *tripleC 12*(2), pp. 431-440, http://triplec.at/index.php/tripleC/article/view/606.

de Laat, P.B. (2007), "Governance of open source software: state of the art", *Journal of Management & Governance 11*(2), pp. 165-177.

Lazaro, C. (2008), *La Liberté logicielle. Une ethnographie des pratiques d'échange et de coopération au sein de la communauté Debian,* Louvain-la-Neuve: Bruylant-Academia.

Levy, S. (2001), *Crypto. How the Code Rebels Beat the Government—Saving Privacy in the Digital Age,* New York: Viking.

Loveluck, B. (2015), *Réseaux, libertés et contrôle. Une généalogie politique d'internet,* Paris: Armand Colin.

MacKenzie, D. & Wajcman, J. eds. (1999), *The Social Shaping of Technology,* 2nd edition, Buckingham: Open University Press.

Mallard, A., Méadel, C. & Musiani, F. (2014), "The paradoxes of distributed trust: peer-to-peer architecture and user confidence in Bitcoin", *Journal of Peer Production* (4), http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewe...

Mathiason, J. (2009), *Internet Governance. The New Frontier of Global Institutions,* London and New York: Routledge.

McLeay, M., Radia, A. & Thomas, R. (2014), "Money release in the modern economy", *Bank of England Quarterly Bulletin* , pp. 14-27.

Mouffe, C. (1993), *The Return of the Political,* London and New York: Verso.

Mouffe, C. & Laclau, E. (2001), *Hegemony and Socialist Strategy. Towards a Radical Democratic Politics,* 2nd edition, London: Verso.

Mueller, M. (2002), *Ruling the Root. Internet Governance and the Taming of Cyberspace,* Cambridge, MA: MIT Press.

Mueller, M. (2010), *Networks and States. The Global Politics of Internet Governance,* Cambridge, MA: MIT Press.

Musiani, F. et al eds. (2016), *The Turn to Infrastructure in Internet Governance,* Basingstoke and New York: Palgrave Macmillan.

Nakamoto, S. (2008a), "Bitcoin: a peer-to-peer electronic cash system", *Bitcoin.org,* https://bitcoin.org/bitcoin.pdf. Accessed 20 February 2014.

Nakamoto, S. (2008b), "Re: Bitcoin P2P e-cash paper", *The Cryptography Mailing List,* http://www.mail-archive.com/cryptography@metzdowd.com/msg09971.html. Accessed 4 May 2016.

Nakamoto, S. (2009), "Bitcoin open source implementation of P2P currency", *P2P Foundation,* http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source. Accessed 15 April 2016.

North, P. (2007), *Money and Liberation. The Micropolitics of Alternative Currency Movements,* Minneapolis, MN: University of Minnesota Press.

Nyman, L. & Lindman, J. (2013), "Code forking, governance, and sustainability in open source software", *Technology Innovation Management Review 3*(1), p. 7.

Olson, M. (1965), *The Logic of Collective Action. Public Goods and the Theory of Groups*, Cambridge, MA: Harvard University Press.

O'Mahony, S. (2003), "Guarding the commons: how community managed software projects protect their work", *Research Policy 32*(7), pp. 1179-1198.

O'Neil, M. (2014), "Hacking Weber: legitimacy, critique, and trust in peer production", *Information, Communication & Society 17*(7), pp. 872-888.

Oram, A. ed. (2001), *Peer-to-Peer. Harnessing the Power of Disruptive Technologies,* Sebastopol, CA: O'Reilly.

Palmer, D. (2016), "Scalability debate continues as Bitcoin XT proposal stalls", *CoinDesk,* http://www.coindesk.com/scalability-debate-bitcoin-xt-proposal-stalls. Accessed 15 April 2016.

Polanyi, K. (2001 [1944]), *The Great Transformation. The Political and Economic Origins of Our Time,* Boston, MA: Beacon Press.

Quinn, B.J. (2009), "The failure of private ordering and the financial crisis of 2008", *New York University Journal of Law and Business* 5(2), pp. 549-615.

Rizzo, P. (2016), "Making sense of Bitcoin's divisive block size debate", *CoinDesk,* http://www.coindesk.com/making-sense-block-size-debate-bitcoin/. Accessed 15 April 2016.

Robles, G. & González-Barahona, J.M. (2012), "A comprehensive study of software forks: dates, reasons and outcomes", in I. Hammouda et al (eds.), *Open Source Systems. Long-Term Sustainability,* Berlin: Springer, pp. 1-14.

Russell, A.L. (2012), "Standards, networks, and critique", *IEEE Annals of the History of Computing 34*(3), pp. 78-80.

Russell, A.L. (2014), *Open Standards and the Digital Age. History, Ideology, and Networks,* Cambridge and New York: Cambridge University Press.

Schweik, C.M. & English, R. (2007), "Tragedy of the FOSS commons? Investigating the institutional designs of free/libre and open source software projects", *First Monday [online] 12*(2), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1619/1534

Scott, B. (2014), "Visions of a techno-Leviathan: the politics of the Bitcoin blockchain", *E-International Relations,* http://www.e-ir.info/2014/06/01/visions-of-a-techno-leviathan-the-politics-of-the-bitcoin-blockchain/. Accessed 2 May 2016.

Shaw, A. & Hill, B.M. (2014), "Laboratories of oligarchy? How the iron law extends to peer production", *Journal of Communication 64*(2), pp. 215-238.

Simmel, G. (2004), *The Philosophy of Money,* 3rd enlarged edition, London and New York: Routledge.

Star, S.L. (1999), "The ethnography of infrastructure", *American Behavioral Scientist 43*(3), pp. 377-391.

Star, S.L. & Strauss, A. (1999), "Layers of silence, arenas of voice: the ecology of visible and invisible work", *Computer Supported Cooperative Work (CSCW) 8*(1-2), pp. 9-30.

Stewart, D. (2005), "Social status in an open-source community", *American Sociological Review 70*(5), pp. 823-842.

The Economist (2016), "Craig Steven Wright claims to be Satoshi Nakamoto. Is he?", http://www.economist.com/news/briefings/21698061-craig-steven-wright-claims-be-satoshi-nakamoto-bitcoin. Accessed 2 May 2016.

Trautman, L.J. (2014), "Virtual currencies; Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?", *Richmond Journal of Law and Technology 20*(4).

von Neumann, J. & Morgenstern, O. (1953 [1944]), *Theory of Games and Economic Behavior*, 3rd edition, Princeton, NJ: Princeton University Press

Winner, L. (1980), "Do artifacts have politics?", *Daedalus 109*(1), pp. 121-136.

Wright, A. & De Filippi, P. (2015), "Decentralized blockchain technology and the rise of lex cryptographia", *Available at SSRN*, http://ssrn.com/abstract=2580664

Zhu, B., Jajodia, S. & Kankanhalli, M.S. (2006), "Building trust in peer-to-peer systems: a review", *International Journal of Security and Networks 1*(1-2), pp. 103-112.

FOOTNOTES

1. See also Oram 2001. The case of file-sharing and its effects on copyright law have been particularly salient (David, 2010).

2. See Hughes, 1993; Levy, 2001.

3. In a fractional-reserve banking system, commercial banks are entitled to generate credits, by making loans or investment, while holding reserves which only account for a fraction of their deposit liabilities – thereby effectively creating money *out of thin air*. A report from the Bank of England estimates that, as of December 2003, only 3% of the money in circulation in the global economy was represented by physical cash (issued by the central bank), whereas the remaining 97% is made up of loans and co-existent deposits created by private or commercial banks (McLeay, Radia, & Thomas, 2014).

4. "[Bitcoin is] completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts… With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless." (Nakamoto, 2009).

5. On 7 November 2008, Satoshi Nakamoto explained on the Cryptography mailing list that *[we will not find a solution to political problems in cryptography,] but we can win a major battle in the arms race and gain a new territory of freedom for several years. Governments are good at cutting off the heads of a centrally controlled network like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own* (Nakamoto 2008b).

6. The double-spending problem is a problem commonly found in many digital cash systems, whereby people can spend the same digital token twice by simply duplicating it. It is usually solved through the introduction of a centralised (trusted) third party, which is in charge of verifying that every transaction is valid, before authorising it.

7. Unless one or more colluding parties control over 51% of the network. See below for a more detailed explanation of the Bitcoin security model.

8. Of course, a variety of tools can be used to reduce the degree of transparency inherent in the blockchain. Just like public-key encryption has enabled more secure communications on top of the internet network, specific cryptographic techniques (such as homomorphic encryption and zero-knowledge proofs) can be used to conceal the content of blockchain-based transactions, without reducing the verifiability thereof. The most popular of these technologies is Zerocash, a privacy-preserving blockchain which relies on zero-knowledge proofs to enable people to transact on a public blockchain without disclosing neither the origin, the destination, nor the amount of the transaction.

9. In October 2009, Bitcoin was first estimated with an exchange rate of 1 USD for 1,309 BTC by the New Liberty Standard, calculated according the costs of electricity that had to be incurred in order to generate bitcoins at the time.

10. The first commercial Bitcoin transaction known to date is the purchase by a Florida-based programmer, Laslo Hanyecz, of a pizza purchased (by a volunteer) from Papa John's for a face value of 10,000 BTC.

11. Over the years, several people have been outed as being Satoshi Nakamoto – these include: Michael Clear (Irish graduate student at Trinity College); Neal King, Vladimir Oksman and Charles Bry (who filed a patent application for updating and distributed encryption keys, just a few days before the registration of the bitcoin.org domain name); Shinichi Mochizuki (Japanese mathematician); Jed McCaleb (founder of the first Bitcoin exchange Mt. Gox); Nick Szabo (author of the *bit gold* paper and strong proponent of the notion of "smart contract"); Hal Finney (a well-known cryptographer who was the recipient of the first Bitcoin transaction); and Dorian Nakamoto (an unfortunate case of homonymy). Most recently, Craig Steven Wright (an Australian computer scientist and businessman) claimed to be Satoshi Nakamoto, without however being able to provide proper evidence to support his claim (2016). To date, all of these claims have been dismissed and the real identity of Satoshi Nakamoto remains a mystery.

12. The Bitcoin Foundation has been heavily criticised due to the various scandals that its board members had been associated with. These include: Charlie Shrem, who had been involved in aiding and abetting the operations of the online marketplace Silk Road; Peter Vessenes and Mark Karpeles, who were highly involved with the scandals of the now defunct Bitcoin exchange Mt. Gox; and Brock Pierce, whose election in spite of his questionable history in the virtual currency space has created huge controversy within the Bitcoin Foundation, eventually leading to the resignation of nine members.

13. In general, forks can be categorised into *soft* and *hard* forks: the former retains some compatibility or interoperability with the original software, whereas the latter involves a clear break or discontinuity with the preceding system.

14. For instance, one of the largest US Bitcoin wallet and exchange company, Coinbase, was removed from Bitcoin.org upon making the announcement that they would be experimenting with Bitcoin XT.

15. As of 11 January 2016, only about 10% of the blocks in the Bitcoin network had been signed by XT nodes (Palmer, 2016).

16. Mike Hearn, interview with the authors, April 2016.

17. a. b. Patrick Murck, interview with the authors, April 2016.

18. Peter Todd and Pindar Wong, interview with the authors, April 2016.

19. See supra, part I.A.

20. This reveals a significant bias of the Bitcoin community towards technological determinism – a vision whereby technological artefacts can influence both culture and society, without the need for any social intervention or assimilation (Bimber, 1994).

21. As the name indicates, the Proof-of-Work algorithm used by Bitcoin requires a certain amount of work to be done before one can record a new set of transactions (a block) into Bitcoin's distributed transaction database (the blockchain). In Bitcoin, the work consists in finding a particular nounce to be embedded into the current block, so that processing the block with a particular hash function (SHA-256) will result in a string with a certain number of leading zeros. The first one to find this nounce will be able to register the block and will therefore be rewarded with a specific number of bitcoins (Nakamoto 2008a). The amount of work to be done depends on the number of leading zeros necessary to register a block – this number may increase or decrease depending on the amount of computational resources (or

hashing power) currently available in the network, so as to ensure that a new block is registered, on average, every 10 minutes. While this model was useful, in the earlier stages of the network, as an incentive for people to contribute computational resources to maintain the network, the Proof-of-Work algorithm creates a competitive game which encourages people to invest more and more hashing power into the network (so as to be rewarded more bitcoins), ultimately resulting in a growing consumption of energy.

22. The difficulty of said mathematical problem is dynamically set by the network: its difficulty increases with the amount of computational resources engaged in the network, so as to ensure that one new block is registered in the blockchain, on average, every 10 minutes.

23. In the early days, given the limited number of participants in the network, mining could be easily achieved by anyone with a personal computer or laptop. Subsequently, as Bitcoin's adoption grew and the virtual currency acquired a greater market value, the economic incentives of mining grew to the point that people started to build specific hardware equipments (ASICs) created for the sole purpose of mining, making it difficult for people to mine without such specialised equipment. Note that such an evolution had actually been anticipated by Satoshi Nakamoto himself, who wrote already in 2008 that, even if "at first, most users would run network nodes, [...] as the network grows beyond a certain point, [mining] would be left more and more to specialists with server farms of specialized hardware."

24. Bitcoin mining pools are a mechanism allowing for Bitcoin miners to pool their resources together and share their hashing power while splitting the reward equally according to the amount of shares they contributed to solving a block. Mining pools constitute a threat to the decentralised nature of Bitcoin. Already in 2014, one mining pool (GHash) was found to control more than half of Bitcoin's hashing power, and was thus able to decide by itself which transactions shall be regarded as valid or invalid – the so-called 51% attack. Today, most of the hashing power is distributed among a few mining pools, which together hold over 75% of the network, and could potentially collude in order to take over the network.

25. Note that the longest chain is to be calculated by taking into account the number of transactions, rather than the number of blocks. The reason for such an arbitrary choice is that the longest chain is likely to be the one that required the greater amount of computational resources, and is therefore – probabilistically – the less likely to have been falsified or tampered with (e.g. by someone willing to censor or alter the content of former transactions).

26. Selfish mining is the process whereby one miner (or mining pool) does not broadcast the validated block as soon as the solution to the mathematical problem for this blockchain has been found, but rather continues to mine the next block in order to benefit from the first-mover advantage in terms of finding the solution for that block. By releasing validated blocks with a delay, ill-intentioned miners can therefore attempt to secure the block rewards for all subsequent blocks in the chain, since – unless the network manages to catch up with them – their fork of the blockchain will always be the longest one (and thus the one that required the most Proof-of-Work) and will thus be the one that will ultimately be adopted by the network (Eyal & Sirer, 2014).

27. Selfish miners encourage honest, but profit-maximising nodes to join the coalition of non-cooperating nodes, thus eventually making the network more vulnerable to a 51% attack.

28. Mt. Gox was one of the largest Bitcoin exchanges, handling over 70% of all bitcoin transactions as of April 2013. Regulatory issues brought Mt. Gox to be banned from the US

banking system, thus making it harder for US customers to withdraw funds into their bank accounts. On 7 February 2014, Mt. Gox halted all bitcoin withdrawals, claiming that they had encountered issues due to the "transaction malleability" bug in the Bitcoin software (which enabled people to pretend a transaction did not occur, when it actually occurred, so as to bring the client to create an additional transaction). On 24 February, the Mt. Gox website went offline and an (allegedly leaked) internal document got released showing that Mt. Gox had lost 774,408 bitcoins in an (allegedly unnoticed) theft that had been going on for years. On 28 February, Mt. Gox filed for bankruptcy reporting a loss of US 473 million dollars in bitcoin.

29. These include, amongst others, the Bitcoin Saving and Trust bitcoin-based Ponzi scheme; the hacking of exchanges such as Bitcoinica, BitFloor, Flexcoin, Poloniex, Bitcurex, etc; or even online Bitcoin wallet services such as Inputs.io and BIPS.

30. *BIP stands for Bitcoin Improvement Proposal. A BIP is a design document providing information to the Bitcoin community, or describing a new feature for Bitcoin or its processes or environment. The BIP should provide a concise technical specification of the feature and a rationale for the feature. We intend BIPs to be the primary mechanisms for proposing new features, for collecting community input on an issue, and for documenting the design decisions that have gone into Bitcoin. The BIP author is responsible for building consensus within the community and documenting dissenting opinions.*
(https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki)

31. https://github.com/bitcoin/bips/blob/master/README.mediawiki

32. "Bitcoin governance is mainly dominated by veto power, in the sense that many parties can choose to stop a change; we haven't seen much use of power to push through changes. The main shortcoming is users have, in practice, less veto power than they should due to coercion." (Peter Todd, interview with the authors, April 2016).

33. "If multiple competing implementations of the Bitcoin protocol exist, mining pool operators and wallet providers must decide which code to run. Their decision is disciplined and constrained by market forces. For mining pool operators, poor policy decisions can lead miners to withdraw hashing power from the pool. Wallet providers may find users shift their keys to another provider and exchange services may find liquidity moves to other providers. This structure favors stability, resilience and a conservative development process. It also makes the development and standards setting process resilient to political forces." (Patrick Murck, interview with the authors, April 2016).

34. The first kinds of physical Bitcoin wallets consisted of a pre-loaded Bitcoin account whose private address was stored in the shape of physical coins that people could hold.

35. As detailed above in Part I.A.

36. Mike Hearn, Pindar Wong, and Patrick Murck, interview with the authors, April 2016.

37. Peter Todd, interview with the authors, April 2016.

38. For instance, what happens when the freedom of expression made possible by the network impinges on country-specific laws? And who should decide (and on what grounds) whether the new .amazon generic Top Level Domain (gTLD) should be attributed to the US American company which has trademarked the name, or to the Brazilian government which lays claim to a geographical area?