INTERNET POLICY REVIEW
Journal on internet regulation

Volume 7 | Issue 4

After the (virtual) gold rush: is Bitcoin more than a speculative bubble?

Maxime Lambrecht
Université catholique de Louvain, Belgium, maxime.lambrecht@uclouvain.be

Louis Larue
Université catholique de Louvain, Belgium, louis.larue@uclouvain.be

Published on 30 Oct 2018 | DOI: 10.14763/2018.4.1353

Abstract: How promising is Bitcoin as a currency? This paper discusses four claims on the advantages of Bitcoin: a more stable currency than state-backed ones; a secure and efficient payment system; a credible alternative to the central management of money; and a better protection of transaction privacy. We discuss these arguments by relating them to their philosophical roots in libertarian and neoliberal theories, and assess whether Bitcoin can effectively meet these expectations. We conclude that despite its advocates' enthusiasm, there are good reasons to doubt that Bitcoin can fulfill its promises and act as a functioning currency, rather than as a mere speculative asset.

Keywords: Bitcoin, Cryptocurrency, Social justice, Efficiency, Libertarianism

Article information

Received: 04 Jan 2018 **Reviewed:** 08 Oct 2018 **Published:** 30 Oct 2018

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/after-virtual-gold-rush-bitcoin-more-speculative-bubble

Citation: Lambrecht, M. & Larue, L. (2018). After the (virtual) gold rush: is Bitcoin more than a speculative bubble?. *Internet Policy Review*, *7*(4). DOI: 10.14763/2018.4.1353

Acknowledgements: The authors wish to thank Primavera de Filippi, Clément Fontan, Olivier Perreira, Mikael Petitjean, Joakim Sandberg, Danielle Zwarthoed, Pierre-Etienne Vandamme and the journal reviewers for their insightful comments and suggestions on this article.

INTRODUCTION

While alternative currencies have always circulated along the main official currencies (Blanc, 2000), a new wave of currencies has emerged, bringing about important changes to the way that we conceive money. Relying on cryptography and peer-to-peer networks, these "cryptocurrencies" neither rest on a central authority nor require any centralised management

or system of payment. In the wake of criticisms of the contemporary banking system following the 2007 financial crisis, they have gained in popularity, and have been presented as an alternative to the current payment system.

Having inspired a great number of alternative cryptocurrencies such as Ripple, Dogecoin, Ethereum, etc [1], Bitcoin remains the most prominent cryptocurrency in terms of valuation and public recognition [2]. Bitcoin has been the subject of much enthusiasm, billed by some as "the future of money" (Frisby, 2014), or presented as "challenging the global economic order" (Vigna and Casey, 2016). Its proponents are often highly critical of state regulations over money, sometimes conceived as inadmissible infringements on freedom, or as inefficient, unsecure, and inflationary (Nakamoto, 2008, 2009).

Naturally, Bitcoin has also attracted a fair amount of skepticism, some going as far as denying that Bitcoin really constitutes a form of money (Dodd, 2017; Glaser et al., 2014; Yermack, 2013), or noting that the Bitcoin valuation exhibits all the characteristics of a speculative bubble (Dwyer, 2015). Moreover, a substantial amount of commentary on Bitcoin focuses on its technical functioning, or on discussing the achievements and flaws of its underlying technology (see for instance Böhme et al., 2015).

Our aim in this article is different. We will avoid dwelling too long on how the technology behind Bitcoin works, nor enter into the discussion as to whether Bitcoin is indeed a form of money. We want to take Bitcoin's proponents at their word: if we consider Bitcoin as a form of money, is it appropriate for use as a currency? Moreover, Bitcoin is often hailed for its supposed advantages over official currencies, the conventional payment system, such as being more stable, safe and efficient, or in allowing to dispense with the need of a central authority. But can it effectively meet these expectations? And if not, is there more to Bitcoin than a speculative bubble? This is what we are going to discuss in this article.

After a brief introduction to Bitcoin for those not already familiar with its technical underpinnings (1), this article reviews four separate arguments in favour of its adoption (2): namely that Bitcoin can be a more stable currency, achieve a more secure and efficient payment system, provide a credible alternative to the central management of money, or better protect transaction privacy. We discuss the philosophical background of these arguments by showing how they relate to the principles of justice developed by libertarians such as Nozick (1974) and Rothbard (2016), and neoliberal economists such as Hayek (1990 [1976]) and Friedman (1959, 1969). The third section of the article then assesses whether Bitcoin can effectively fulfil these expectations (3). First, we will consider whether Bitcoin's design makes it a stable currency; (3.1). Second, we question the security and efficiency of Bitcoin's payment system; (3.2). Third, we discuss the issue of whether Bitcoin can indeed function as a radically decentralised currency, free from centralised governance or authority (3.3). Finally, we address the extent to which Bitcoin can protect payment privacy (3.4). We conclude that it is unlikely that Bitcoin can function as a currency unless it changes drastically, which would probably detract from the characteristics that make it attractive to its proponents.

1. WHAT IS BITCOIN?

Whether Bitcoin is, or is not, a form of money is still a highly debated issue (Bjerg, 2016; Urquhart, 2016; Glaser et al., 2014; Yermack, 2013). Of course, the definition of money is itself a controversial issue. Money is sometimes conceived as a debt token (Graeber, 2011), as a social

relation (Ingham, 2004), as a social totality (Aglietta and Orléan, 2002), or as a peculiar social convention fulfilling a certain number of functions (Tobin, 2008), among other examples. Despite their divergences, most theories of money generally recognise that, in modern societies, money is a medium of exchange that is widely accepted within a specific community. [3] This definition will suffice for the purpose of this article. In this article, we will assume that Bitcoin can indeed be considered as a form of money, as our goal is to determine whether, as a currency, it can fulfil certain specific aims or functions.

Bitcoin differs in many respects from "official currencies" such as the Euro or the Dollar. Coins and notes are usually emitted by the Central Bank of each monetary zone (the European Central Bank for the Eurozone, the US Federal Reserve for the Dollar), while deposit money, which constitutes the vast majority of money supply today, is made up of funds held in demand deposit accounts in commercial banks (McLeay, Radia, and Thomas, 2014).

By contrast, Bitcoin is a decentralised cryptocurrency that rests on a distributed repository, protected and managed through the use of cryptographic protocols. It is thus independent from any central authority.

First, Bitcoin is not backed by a State or a Central Bank. Contrary to the Euro or the Dollar, where a Central Bank is in charge of ensuring price stability and financial stability through adequate monetary policy (Goodhart, 2011; Goodhart et al., 2014), there is no such central authority in the Bitcoin system. There is no lender of last resort either, that is, a State or a Central Bank that could bail out banks in the event of a financial panic (Goodhart, 1991; Blinder, 2010).

Second, Bitcoin's payment system is entirely decentralised and rests on an open-source cryptographic protocol. This protocol originates from an article published in 2008 by a certain Satoshi Nakamoto (2008), whose identity remains mysterious (Davis, 2011). The central innovation of Bitcoin, which puts together previous advances in cryptography, such as the proof of work technology (Narayanan and Clark, 2017), is that it is based on a decentralised public ledger (Ali et al., 2014a). In a conventional payment system, banks hold a record of transactions and ensure that no unit of money is used more than once by the same user ("double-spending" problem). With Bitcoin, this control system is decentralised through a public ledger system operated on a peer-to-peer network. This ledger has several important properties. First, every user can verify and process transactions. Moreover, the Bitcoin protocol secures the ledger against falsifications, without resorting to any banking institution or any central authority. Finally, an important consequence of the public availability of this ledger is that Bitcoin can only preserve a "pseudo-anonymity" for its users: details of all transactions are logged on the public ledger, where the only indication of the identity of their parties is their Bitcoin address (Luu and Imwinkelried, 2015).

A third crucial difference between Bitcoin and conventional currencies lies in its creation process. Every user can participate in the creation of new Bitcoins, by resolving a deliberately complicated series of algorithms (though in practice this "mining" process is mainly taken up by professional miners). The first Bitcoins were created from scratch and used by the first Bitcoin users. The first user of the protocol, assumed to be Nakamoto himself, mined the first 50 Bitcoins in 2009 (Wallace, 2011). The following Bitcoins are created when new transactions take place, as a reward going to those who successfully add a new block to the ledger. More precisely, miners, by solving puzzles, try to verify each transaction and to get the right to add it to a new "block" containing several transactions, appended in the Bitcoin ledger (also called the "Blockchain", for that reason). This new block is accepted within the ledger if it contains a valid

transaction and a new puzzle solution. Miners are all competing to verify each transaction in order to get the reward attached to the completion of a block. Along with this reward, miners may also set a fee for processing transactions, as a complementary revenue. While at the start these fees were marginal, they have tended to rise steeply recently due to network congestion, which led to a major crisis about reforming the protocol (see section 3.1). Eventually, every time a block is verified, new Bitcoins are minted. [4]

However, this Bitcoin creation process has an algorithmic limit. The Bitcoin protocol has a marginally decreasing rate of Bitcoin creation per block, which approximates the rate at which gold is mined. Therefore, the total supply of Bitcoins will asymptotically approach the amount of 21 million (Houy, 2014), which, according to some estimations, will be reached around the year 2140 (Ali et al., 2014a). The reward of miners is therefore set to decrease, being divided by two every 210,000 blocks, while the difficulty of mining is programmed to increase along with the network size. Nowadays, more than 17 million Bitcoins have been mined (according to blockchain.info, consulted 19/07/2018). Approximately 200,000 transactions take place every day, for an estimated value of less than 1 million BTC.

2. THE CASE FOR BITCOIN ADOPTION

Bitcoin's proponents do not form a homogeneous group, and many people may support Bitcoin adoption for different reasons. However, the main recurring cases for Bitcoin adoption may be summarised as follows:

- Bitcoin can constitute a more stable currency than conventional state-sponsored money, by taking monetary policy out of the government's hands
- Bitcoin can provide a more secure and efficient payment system compared to a system relying on trusted third parties
- Bitcoin can dispense with the need of coercive institutions such as States and Central Banks, by achieving a decentralised securing of transactions through cryptographic proof
- Bitcoin helps protect users' privacy against abuse of state power through government surveillance

First, Bitcoin is often hailed as a means to achieve a more stable monetary system (Ametrano, 2016; Collard, 2017; Lakomski-Laguerre and Desmedt, 2015; Rochard, 2013). As Nakamoto (2009) stresses, with conventional currencies, "the central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust". As others have noted (ECB, 2012, p. 23), this criticism reminds the neoliberal critique that state monopoly in the issuance of money will necessarily lead to over-inflation, resulting in depressions and unemployment (Hayek, 1990 [1976]; Friedman, 1959, 1969). Hayek argued that governments have a tendency to abuse their monopoly power by systematically creating too much money (Hayek, 1990 [1976], pp. 28–32). Similarly, Friedman and Schwartz (1963) argue that historically, interventions of the Federal Reserve of the United States have been mostly detrimental to economic stability and have often worsened crises rather than solved them. Even if this account has been contested (Kindleberger, 1973, 1978), Friedman argues on this basis that monetary policy should "avoid sharp swings" (Friedman, 1968, 15) and proposed to "freeze" the monetary base by setting a fixed rate of growth in the amount of money (around 3–5% according to Friedman (1959, p. 91, 1968, p. 16)). His argument is based on historical evidence, but also on his own theory, which, similarly to Hayek's ([1976] 1990), predicts that excessive money creation is inflationary and cannot impact employment in the long run (Friedman, 1968).

The Bitcoin protocol is designed in this spirit and has been praised for its "perfect monetary policy" (Rochard, 2013): since no central agencies can control the Bitcoin's supply, whose rate of growth is set algorithmically, it is immune from inflation. Actually, unless a majority of nodes decides collectively to modify the protocol itself, there is no procedure for altering the rate of Bitcoin creation. It is not our purpose in this article to discuss the economic merits of such a fixed or "algorithmic" monetary policy, an issue which is the subject of an extensive literature (see Bordo, 2008, for a review of the recent debates). However, as we shall see in section 3, to really fulfill that promise, Bitcoin must be able to dispense with any central governance altogether and it is doubtful that it could, while retaining the other qualities that would make it an attractive currency.

Second, Bitcoin is often presented as the basis for a more secure and efficient payment system, which allows to dispense altogether with the need for a trusted third party (Ali et al., 2014a; Angel and McCabe, 2015; Grinberg, 2011; Vidan and Lehdonvirta, 2018). According to Angel and McCabe (2015, p. 606), Bitcoin "represents a technological solution that creates appropriate incentives for honesty without needing a government to enforce laws against dishonesty." This motivation originally comes from a distrust of banking institutions, which, in the context of the 2008 global financial crisis, many consider as unsafe (Ali et al., 2014a, p. 6; Maurer et al., 2013, pp. 261–262). Presenting Bitcoin in the aftermath of the crisis, Nakamoto (2009) has some harsh words for our current banking system, where "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". Bitcoin's payment system is presented as safer, since it does not require trusting any particular payment intermediary. Moreover, Nakamoto also points to two other disadvantages of having to rely on a trusted third-party: the transaction costs it induces, as well as the possibility of fraud through reversal of transactions (see also Angel and McCabe, 2015, p. 606). By providing "a system based on cryptographic proof instead of trust", Bitcoin purports to reduce transaction costs due to the absence of intermediary, and reduce opportunities for fraud by making transaction irreversible (Nakamoto, 2008, p. 1).

A third argument contends that Bitcoin may contribute to lessening the level of state coercion facing individuals, by putting money out of the control of government or any centralised institution. Indeed, another common objection to the exercise of monetary policy by states, besides stability, stems out of a libertarian concern for the protection of the rights and liberties of individuals (Nozick, 1974; Rothbard, 2016). Safeguarding these rights and liberties puts limits on what others can legitimately do to people without their consent. The State should keep only a marginal role, which basically consists of protecting property rights from theft or fraud. Apart from that, state interventions in the economy encroach on individual freedom (i.e., coercion), and is therefore wrong. This argument clearly rejects the possibility of the State's monopoly over money. In the words of Murray Rothbard, such a monopoly allows the State to act as a "legalized, monopoly counterfeiter" and use monetary creation as "a giant scheme of hidden taxation", therefore violating individual property rights (Rothbard, 2016). Similarly, for Hayek, "legal tender is simply a legal device to force people to accept in fulfilment of a contract something they never intended" (Hayek, 1990 [1976], pp. 39–40). It thus violates their freedom to set voluntarily the terms of a contract.

Libertarianism constitutes an important philosophical root among Bitcoin proponents (Golumbia, 2016; Karlstrom, 2014; Lakomski-Laguerre and Desmedt, 2015; Wallace, 2011). For libertarians, such as Dowd (2014, p. 64), Bitcoin safeguards "the freedom of the individual to trade, and the freedom of the individual to accumulate, move and protect his or her financial wealth — in other words, financial freedom." Because it supposedly allows to dispense with the

need for any central institution, Bitcoin may significantly weaken the hold of coercive institutions over individuals' lives.

Bitcoin's fourth alleged advantage flows from the previous one: because Bitcoin's payment system (supposedly) does not rely on trusted intermediaries, it would better protect the privacy of its users than conventional means of payments. For instance, Nakamoto (2009) complains that "we have to trust [banks and payment intermediaries] for our privacy [and] trust them not to let identity thieves drain our accounts". In the aftermath of the NSA surveillance scandals (Hintz, 2014), which has showed that private intermediaries could rarely be trusted to protect the privacy of their customers against overreaching state authorities, privacy has often been viewed as one of Bitcoin's main appeal.

However, the extent to which Bitcoin can fulfil these promises is doubtful, as we will discuss in the following section. Indeed, while Bitcoin's distributed cryptographic proof is an important technical achievement with interesting potential applications, basic market analysis makes it dubious that Bitcoin's promise to act as a reliable non-inflationary currency is really sustainable (section 3.1). Moreover, there are reasons to be wary of its claim to provide a more secure and efficient means of payment, due to the prevalence of intermediaries and transaction costs (section 3.2). Besides, Bitcoin's decentralised architecture, while making it independent from central governance from Banks or States is also what makes it extremely difficult for its community of developers and users to govern it (section 3.3). Finally, it is highly unlikely that Bitcoin can meet the expectations of users who regard it as a way to better protect the privacy of their transactions, and even if it did, it would raise serious concerns for the possibility of law enforcement and redistribution (section 3.4).

3. CAN BITCOIN FULFIL ITS PROMISES?

3.1. IS BITCOIN A STABLE CURRENCY?

One of Bitcoin's main promises is to provide a more stable currency than conventional, State-backed money, that would not be plagued by the States' or Central Banks' inflationary biases, or otherwise nefarious monetary decision.

However, even if Bitcoins were more widespread in the population, day-to-day use of Bitcoin as a currency would still face important hurdles, due to its high volatility compared to other currencies. Indeed, this volatility undermines its quality both as a means of exchange and as a store of value.

Bitcoin's volatility is well illustrated by the following graphs (Figures 1, 2, and 3), which show that Bitcoin's price has gone up and down between 2013 and the present day. Figure 1 illustrates how the market price of a Bitcoin has sharply risen from around five dollars in 2011 to an all-time high of $19,783 by the end of 2017. However, due to the scale of this graph, it fails to accurately depict how Bitcoin's value has varied on a day-to-day basis. To better illustrate Bitcoin's volatility, it is useful to represent this data in two additional close-up graphs. Figure 2 is limited to the pre-2017 period, while Figure 3 focuses on the period between January 2017 and the present day.

Financial economists have studied Bitcoin's volatility in depth. Dwyer (2015) finds that Bitcoin's average volatility is always higher than for gold or a set of foreign currencies. Cheah and Fry (2015) and Cheung, Roca, and Su (2015) show, using econometric models, that the price of

Bitcoin exhibits speculative bubbles. These studies show how, for many users, Bitcoin is mainly used as a speculative asset, which people buy and sell for the sake of rapid financial profit, explaining why, as a consequence, its value has varied sharply throughout time. This has led some to conclude that Bitcoin is a financial asset rather than a currency (Glaser et al., 2014; Urquhart, 2016; Yermack, 2013).

Why does volatility matter? First, a volatile asset is a less secure asset, from an investor's point of view. Contrary to gold or government bonds, it might yield a greater return, but bears the risk of abruptly losing its value. Second, volatility means that one cannot predict the future value of a commodity (labeled in Bitcoin), which tends to fluctuate constantly and in a random way. This means that Bitcoin cannot be a stable unit of account as it is unable to represent adequately the value of goods and services. Volatility exacerbates uncertainty and undermines the possibility of contracting in Bitcoin, which cannot, therefore, constitute a reliable means of exchange and a secure store of value.

In sum, the empirical evidence from Bitcoin's financial records appears to contradict the claim that Bitcoin can provide a stable means of payment and store of value, in line with the theoretical prescriptions of Friedman and Hayek.

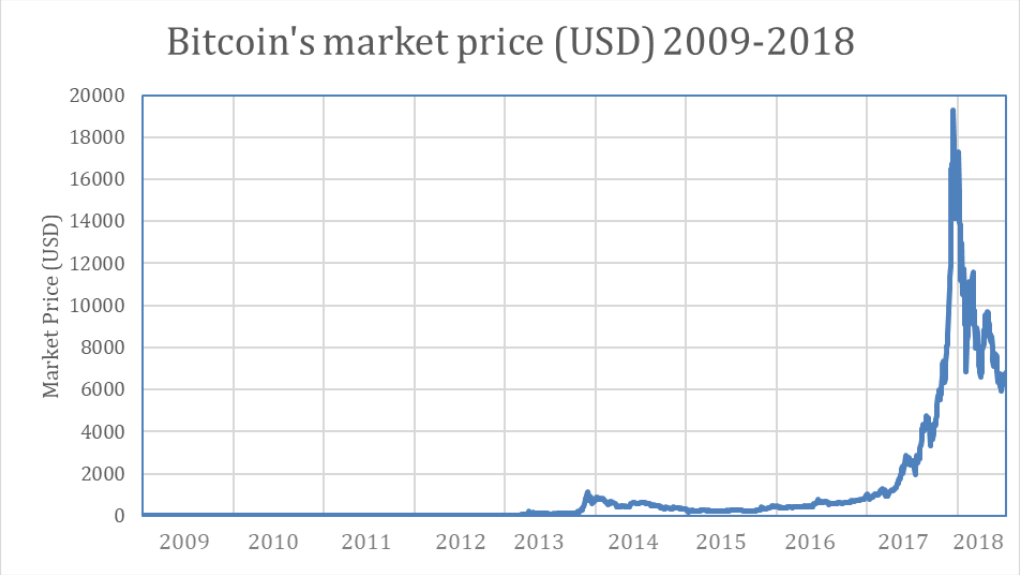

Figure 1: Bitcoin's market price 2009–2018 (source: Own elaboration based on data collected on blockchain.info)

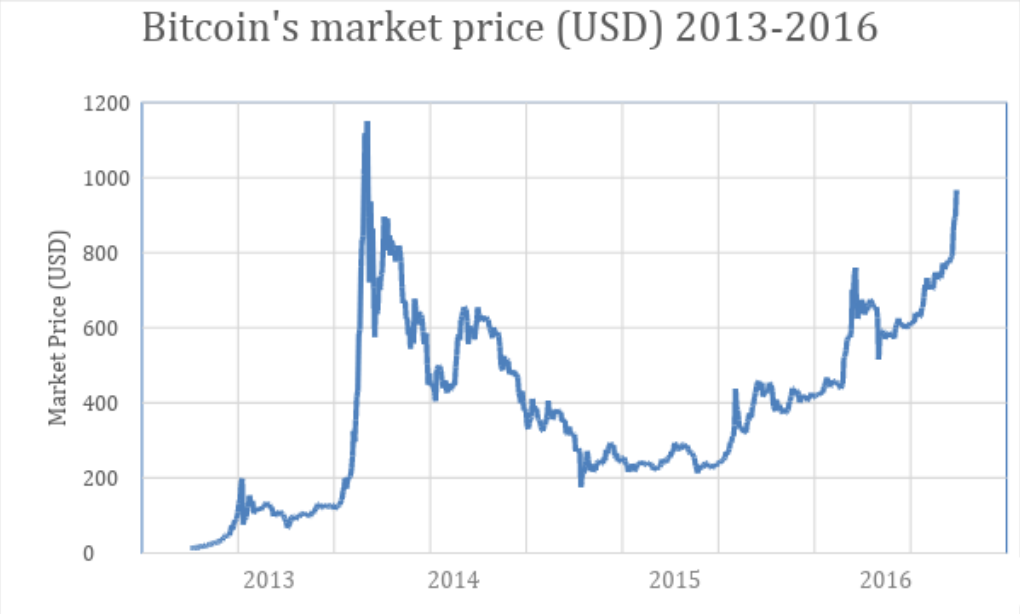

Figure 2: Bitcoin's market price 2013–2016 (source: Own elaboration based on data collected on blockchain.info)

Figure 3: Bitcoin's market price 2017–present (source: Own elaboration based on data collected on blockchain.info)

3.2 IS BITCOIN A SECURE AND EFFICIENT PAYMENT SYSTEM?

A second argument in favour of Bitcoin adoption contends that it is a more secure and efficient means of payment and store of value than conventional money, as its payment system does not rest on centralised institutions, such as Banks.

However, while Bitcoin's protocol itself has been remarkably secured against possible abuses or manipulations, this security is undercut by the difficulty for users of securing their Bitcoins against fraud or loss. Indeed, Bitcoin users are faced with a dilemma between ensuring their own security, and trusting intermediary services. Storing one's wallet on one's computer is not much different than keeping one's money in a safe: unsecure password can be cracked, stolen through "phishing" scams, or simply forgotten. And because Bitcoin transactions are non-

reversible, victims are left without recourse in case of theft (Guadamuz and Marsden, 2015, p. 10).

Therefore, for many users online wallet services and even Bitcoin exchanges can appear as safer alternatives for storing and trading one's Bitcoins, just as Banks are considered safer than keeping one's money in safes. However, if one resorts to such online intermediaries, Bitcoin is not any more secure than conventional currencies, where one has to rely on banking and payment intermediaries. It can even be even less secure, as few of these services are (for the moment) regulated beyond the usual protection of general contract and insolvency law (the main focus of legislators having been the use of cryptocurrencies for money laundering [5]). Users of cryptocurrencies are therefore left without much protection against fraud or bankruptcy. The bankruptcy of MtGox, one of the prominent Bitcoin exchange platforms (where Bitcoins can be traded-in for national currencies), has shed light on the risks taken by Bitcoin holders (Popper and Abrams, 2014). The collapse of MtGox was partly due to technological incidents, and to an apparent theft of no less than 744,000 Bitcoins, valued approximately at $350 million at the time (Popper and Abrams, 2014). This illustrates how Bitcoin's users are highly vulnerable to frauds or to bankruptcies affecting exchange platforms. As the European Banking Authority rightly highlights, "no specific regulatory protections exist that would cover you for losses if a platform that exchanges or holds your virtual currencies fails or goes out of business" (European Banking Authority, 2013, p. 1). On the contrary, centralised payment systems, such as the Euro system, are partly protected from such events. In Belgium, for instance, banking deposits are guaranteed by the State up to €100,000 per person. [6] Of course, the protection of deposits differs from the protection of payments. However, the fact that deposits are protected is an indirect protection of payments: people are ensured that their money is safe (or a large part of it) and the continuity of payments is therefore guaranteed. Moreover, states usually play the role of lender of last resort. If banks go bankrupt, that is, if they cannot honour their debts any more, States can usually bail them out to avoid a collapse of the economy. These two kinds of protection are absent from the Bitcoin's payment system, which exposes users to frauds and to bankruptcies of exchange platforms.

Another difficulty for Bitcoin to act as an efficient means of payment is the issue of transaction costs. While Bitcoin speed and low transaction fees were advocated among the cryptocurrency's assets compared to traditional banking solutions, Bitcoin's scaling problem due to rising user adoption (which we will cover more extensively in the next section) has radically changed the equation.

Indeed, the congestion in the Bitcoin network led to a sharp rise in transaction fees. While for most of the cryptocurrency's history users have enjoyed negligible transaction fees, the average transaction fee had risen from less than $0.1 in January 2017 to about $4 in June 2017, even (briefly) reaching an all-time high of almost $54 per transaction in mid-December 2017. [7] Confirmation time for transaction had also witnessed a sharp rise: from an average of 20 minutes in August 2016, with a peak at 92 minutes on 16 August, it increased to an average of 123 minutes in August 2017, with a peak at 1,524 minutes on August 27 [8]. Since then, however, the average fee has decreased significantly to less than $1, and the average confirmation time is back to around 20 minutes, as of June 2018.

This return to normal has been attributed to various factors, such as a calming down of Bitcoin's latest speculative bubble of late 2017 (Torpey, 2018) and the adoption of a protocol upgrade called "Segwit" intended to mitigate the issue of block size (Sedgwick, 2018) by packing more payments into less space on the blockchain (Lee, 2018). However, this respite might be

temporary. A future rise in the demand for Bitcoin, and a failure to timely adapt the Bitcoin protocol to this rise, may well lead to higher and more volatile transaction fees. This equation is further complicated by the algorithmic decrease of miners' reward, which is supposed to be offset by an increase in transaction fees (Nakamoto, 2018, p. 4).

To sum up, as of today Bitcoin is still far from providing a secure and efficient means of payment. Admittedly, many actors are trying to address these issues in their attempts of reforming Bitcoin, which is at the heart of the still-ongoing block size debate. Bitcoin users are notably pinning their hopes on a proposed alternative payment network, called the Lightning network, which it is still under development. However, as we will see in the next section (3.3), there are good reasons to entertain serious doubts on the capacity of the Bitcoin community to successfully tackle such technical challenges.

3.3 CAN BITCOIN AVOID FORMAL GOVERNANCE?

As we have seen, for some, one of the main appeals of Bitcoin and other cryptocurrencies lies in their decentralised nature, which minimises the influence of coercive institutions (such as States and Central Banks) on monetary policy. Whatever the merits of the underlying libertarian argument, it is dubious that Bitcoin can dispense altogether with any formal governance or trust in some privileged actors.

Let us begin by noting that the original Bitcoin source code, originally drafted under the name of Satoshi Nakamoto, already contains a great number of substantial rules, which have an effect on the economics of Bitcoin: the decreasing supply of Bitcoins to be minted, the cap on the size of transaction blocks, etc.

Are these rules entirely set in stone, immutable? And if not, who has the power to alter them? This is the issue at the heart of Bitcoin governance. While Bitcoin has indeed no formal governance (there is no constitution or founding principles setting decision-making procedures), a set of practices have emerged, in the interplay of three categories of actors: core developers, miners, and users.

Taking over from Nakamoto's initial drafting of the protocol, the core development team enjoys a sort of moral authority over the community, which entrusts it for technical decisions. Core developers control the GitHub repository (https://github.com/bitcoin/) and the domain (https://bitcoincore.org). As with many open source development projects, Bitcoin follows a "autocratic-mechanistic" model, where anyone is free to contribute code, but a small group of co-opted developers (the core developers) can ultimately decide which changes get implemented in the software (de Laat, 2007; de Filippi and Loveluck, 2016).

However, it is important to note that the Bitcoin core development team cannot impose any modifications to the existing Bitcoin protocol without the consent of at least a substantial number of miners or users. Since Bitcoin is an open source software, any user could refuse to update its software and continue to use its older version, or propose an alternative change to shift the software development in a different direction, thereby creating a "fork" (an alternative branch of a software development). In the case of Bitcoin, this can happen essentially through two mechanisms.

The first is called a "soft fork", and consists in adding stricter rules determining which blocks or transactions are valid. A soft fork can be imposed on the existing network with the collaboration of miners with a mere majority of hash-power, which can enforce the new rules by rejecting blocks or transactions that do not conform to the change.

The second is called a “hard fork”, which touches on the fundamental characteristics of the protocol such as block structure or difficulty rules. As it is not backward-compatible, a hard fork requires all full nodes to upgrade, or the blockchain could split between users using the new updated version and those using the older version.

Finally, in the Bitcoin development community, a standard form of building consensus around a proposed modification has emerged in the form of documents called Bitcoin Implementation Proposals (BIPs).

For a long time, these issues of governance where mostly ignored, primarily due to the idea that the developers’ role was purely technical and unlikely to cause deep ideological divergence (Lehdonvirta, 2016).

In the last few years however, the Bitcoin block size controversy has brought to light the importance of governance and what de Filippi and Loveluck (2016) call the “invisible politics” of Bitcoin. Indeed, a deep disagreement divides the Bitcoin community on the issue of the Bitcoin’s block size cap, a computational bottleneck that has increasingly worsened transaction fees and processing delays with Bitcoin’s gain in popularity. A first risk of split occurred in 2015 when some Bitcoin core developers proposed a fork called “Bitcoin XT”, aiming to increase its block size from 1 to 8 megabytes. After much debate, the Bitcoin community stayed loyal to the original Bitcoin protocol (billed “Bitcoin Core”), thus avoiding a definite split. However, the attempts by the reformists were pursued, and during 2016 and 2017 various fork proposals have been made, either by consortiums of miners or users. To succeed, these reform proposals generally require reaching a particular adoption rate of a qualified majority of miners or users before a given date. While the process is still ongoing, and since only a particular proposal (Segwit) did get adopted, this process remains complex and risky for the integrity of Bitcoin’s blockchain. And indeed, it has already generated its first major split: in August 2017, after months of Bitcoin scaling controversy, a group of users successfully hard-forked Bitcoin, as well as its whole transaction history, into a new cryptocurrency with a block size of 8Mb, named Bitcoin Cash. While the hard fork did not cause the rate of Bitcoin to crash, as some feared, it nonetheless showed that the risk of a Bitcoin schism was a very real possibility.

The risk of schisms can already prove problematic in the context of free and open source software, where forks pose the risk of scattering developers and users between incompatible projects, threatening their sustainability (Robles and González-Barahona, 2012). However, it is even more problematic in the case of a currency, where network effects are crucial (Lehdonvirta, 2016): while a given piece of software can be useful to a very small niche of users, a currency can only function as such if enough people are willing to exchange it or accept it as a means of payment. These schisms could significantly weaken Bitcoin by diminishing its attractiveness as a medium of exchange. Admittedly, until now, the existence of a great number of alternative cryptocurrencies has apparently not curbed user enthusiasm for Bitcoin. However, there is a significant risk that the ongoing multiplication of Bitcoin clones (such as "Bitcoin Cash", "Bitcoin Gold", "Bitcoin Diamond"…) will constitute a factor of confusion for the broader public, thereby threatening its ability to be used as a mainstream medium of exchange.

Therefore, not only is Bitcoin not the self-governing, radically decentralised currency that some of its supporters would want it to be; Bitcoin’s informal governance, plagued by the risk of schisms, also constitutes a significant threat to its sustainability as a currency.

A second significant challenge to the idea that cryptocurrencies can escape governance or central authorities is related to the particular way transaction security is achieved with Bitcoin.

Bitcoin's "proof-of-work" security is crucially based on trusting a majority of nodes in the system: in his 2008 paper, Nakamoto notes that proof-of-work security will be able to resist attackers "as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes" (Nakamoto, 2008, p. 1). Perhaps initially this threshold of 50% seemed high enough, ensuring that it cannot easily be reached. However, in 2014, a consortium (or "pool") of miners called GHash.io was able to concentrate 51% of the total computational power (Goodin, 2014). Therefore, this pool of miners potentially had the ability to circumvent the security of Bitcoin's payment system, and spend the same coins twice or reject competing miners' transactions. That this concentration of power did not last long is due to the care of individual miners, who decided to pull from the pool out of a concern for Bitcoin's integrity. Due to the criticism, the operators of GHash.io issued a statement and committed to "take all necessary precautions to prevent reaching 51% of all hashing power"(Hajdarbegovic, 2014).

Therefore, as others have noted, Bitcoin's central security feature "depends on the goodwill of a few people whose names nobody knows" (Bershidsky, 2014). Can the Bitcoin community rely on the goodwill of individual miners and social responsibility of mining pools to avert an attack? Or should mining pools be prevented to acquire such a position? The latter option would likely involve some kind of antitrust regulation, similar to conventional antitrust laws. It would require, therefore, a sort of central competition authority to prevent collusion among miners.

Consequently, either the Bitcoin community retains its own libertarian form of "governance" by competition between forks, with risks for its governability, user base and security, or it recognises that some degree of formal central governance is inevitable. However, that recognition leads to what Lehdonvirta bills as the "blockchain's governance paradox": if Bitcoin users address the problem of governance by trusting a central institution to make the rules, then why do they need a decentralised cryptocurrency anymore? (Lehdonvirta, 2016).

In summary, the prevailing skepticism against governance among the Bitcoin community has made any change in its algorithmic regulation very difficult and long to achieve, and prevents putting in place any structural protection against a collusion by miners to breach its proof-of-work security. Bitcoin's informal governance model does not fare well compared to its promise to provide a reliable alternative to the allegedly flawed centralised banking system.

3.4 DOES BITCOIN IMPROVE PAYMENT PRIVACY?

Finally, one last perceived advantage of Bitcoin over conventional currencies is the better protection of payment privacy that it is supposed to provide, since its decentralised payment system makes it independent of banks or other payment intermediaries, and does not require disclosure of an account holder's identity. Admittedly, this is not a claim that more knowledgeable Bitcoin proponents are likely to make, as it has been at the centre of much criticism. However, it remains a recurrent preconception, at least in popular opinion and among some Bitcoin users, and therefore deserves a brief discussion here.

There are many good reasons why people might seek privacy in their transactions. They might wish to avoid mass data collection of their transaction history by private companies for targeted marketing, or they can be political opponents, fearing retribution from authoritarian regimes.

However, these privacy-protecting features are also what makes Bitcoin a particularly suitable tool for engaging in fraud, illegal business, and tax evasion, which has been a recurrent concern for lawmakers (Gibbs, 2018; Gruber, 2013; Kollewe, 2018; Marian, 2013; Mersch, 2018).

At the core of the Bitcoin protocol are two distinct features, which have opposite tendencies in

terms of anonymity. On the one hand, Bitcoin's public ledger tends to make it more transparent, as all transactions are logged in a publicly accessible ledger. On the other hand, Bitcoin's peer-to-peer network tends to make it more anonymous (as it does not rely on the presence of financial intermediaries holding all the users' information).

As others have noted, Bitcoin only provides pseudo-anonymity, in that while a given transaction only lists the pseudo-anonymous Bitcoin address of the sender and receiver, details of all transactions are logged on the public ledger. Therefore, as Luu and Inwinkelried (2015, p. 10) put it, "[i]f a Bitcoin address could somehow be associated with a specific identity, the pseudo-anonymity would be penetrated". Parties to a transaction could be traced back to the holder of an exchange account, by using identification techniques such as traffic analysis, and transaction graph analysis (Biryukov, Khovratovich, and Pustogarov, 2014; Luu and Imwinkelried, 2015, p. 24; Reid and Harrigan, 2013, p. 17). State authorities could use such information to identify customers of cryptocurrency exchanges, provided such services are imposed "Know Your Customer" obligations under anti-money laundering regulations, as is the case in the US under the US Department of Treasury's guidance on virtual currencies [9], as well as in the EU with the recent adoption of the 5th Anti-Money Laundering Directive [10]. In the EU, since "virtual currency" exchanges services as well as custodian wallet providers are now covered by the 5th AML directive, they are subject to customers due diligence obligations as well as obligations to report transactions suspected of being the proceeds of criminal activity, or being related to money laundering or terrorist financing.

Therefore, until Bitcoin use become sufficiently widespread that an autonomous Bitcoin economy could be imaginable, the position of gatekeeper held by exchanges in the flow of Bitcoin appear to undercut the claim for Bitcoin to be any more privacy-protecting than conventional currency. Indeed, none is entirely disintermediated, they are just relying on different sorts of financial intermediaries.

A possible way to disrupt this possibility of identification would be to use mixing services (also called "laundry services"), which allow a user to exchange a given amount of tainted Bitcoins for a corresponding sum coming from a multiplicity of other users, and sent to a new Bitcoin address (Gruber, 2013, pp.189–193; Marian, 2013, p. 44). However, the issue with relying on third-party mixing services is that they could themselves be the target of court injunctions, or be the subject of "Know Your Customer" obligations, as with Bitcoin exchanges.

Of course, users could possibly resort to exchanges or mixing services based in lax or lawless jurisdiction, in order to minimise the risk that their data be handed over to the authorities by such services. They would however face an important issue of trust, as those unregulated mixing services are also likely to be the less reliable, with little guarantee of seeing one's money back in case of fraud. This apparently happened to Meiklejohn et al. (2013) while studying these services, who note in their article that "[o]ne of these [mixing services], BitMix, simply stole our money".

Thus, it does not seem that Bitcoin could achieve a better level of transaction privacy than conventional currencies. Some even go so far as arguing that, far from making the job of law enforcement agencies harder, Bitcoin even generates new opportunities to track down illicit activities (Kaplanov, 2012, p. 171). Companies like Chainanalysis have developed software aimed at analysing the blockchain to identify Bitcoin users, which have been used by several public agencies, such as the US Internal Revenue Service, the FBI, or Europol (Orcutt, 2017).

This provides a good reason for State authorities not to ban Bitcoin altogether, for risk of

promoting alternative cryptocurrencies that better protect transaction privacy without resorting to third parties. However, a case could be made that cryptocurrencies embedding protocol-level privacy protection (such as the proposed Zerocash, which would integrate a mixing service in the blockchain itself [11]) should be banned, as they could be used as gateway currencies for transacting in Bitcoin, therefore evading scrutiny by State authorities. Whether such repressive approach is at all feasible remains an open question.

More fundamentally, the decentralised (although not entirely disintermediated) nature of cryptocurrencies like Bitcoin has another important drawback for user privacy: without a bank or financial institution, users are solely responsible for the privacy of their transaction. And the average — not particularly tech savvy — consumer will be more likely to commit some privacy oversight in its Bitcoin transactions. Therefore, paradoxically, the many flaws in Bitcoin's privacy protection mean that unsophisticated users might enjoy a lesser level of transaction privacy by using such a pseudo-anonymous cryptocurrency than by relying on traditional financial intermediaries.

CONCLUSION

Now that the latest Bitcoin "gold rush" appears to have – momentarily – receded, the central question for potential Bitcoin users remains: are there good reasons to adopt Bitcoin, other than investing in a speculative asset?

This article highlighted four arguments justifying the attractiveness of Bitcoin. To recall, the first lies in Bitcoin's practical promise of constituting a stable currency, immune to inflation, in the spirit of what neoliberal authors like Hayek or Friedman have argued for. The second is that Bitcoin could help reducing state coercion by dispensing with the need of a monetary policy, in line with the libertarian ideal of a minimal state. The third argument is that Bitcoin would constitute a more efficient and safe system of payment. And the fourth is that Bitcoin supposedly better protects transaction privacy than the conventional banking system.

As we saw, it is dubious that Bitcoin, as it is now, can deliver on these promises.

First, Bitcoin's financial record detracts from any claim of being a stable currency: its highly volatile value makes it risky for merchants to accept, and inconvenient for consumers to use. This, alone, makes Bitcoin unfit to be used as an alternative currency for the time being.

Second, Bitcoin's promise to provide an efficient store of value or means of payment is not supported by evidence from its use. On the one hand, securely storing and trading one's Bitcoins requires a substantial level of knowledge from its users. On the other hand, consumer confidence in Bitcoin's capacity to provide efficient payment facilities lies on shaky foundations: an increased success of Bitcoin could lead to higher transaction fees and longer confirmation times, which would make it impractical for consumers.

Third, the promise of making Bitcoin a currency independent from central authorities has been largely a double-edged sword. Even if the Bitcoin protocol is an achievement of a currency run by a radically decentralised network, it is highly unlikely that it can act as a reliable and governable currency without some formal governance mechanisms, and without resorting to some financial intermediaries. As exemplified by the ongoing scaling debate, the Bitcoin community's unwillingness to seriously address the issue of Bitcoin governance undermines its resilience to economic and technical challenges. Bitcoin's current informal governance

mechanism generates recurrent risks for its sustainability and integrity, as it creates uncertainty for users as to the value of their holdings as well as to which "fork" of the Bitcoin blockchain constitutes the "real" Bitcoin. Moreover, without formal governance mechanisms, Bitcoin ultimately relies on trusting the goodwill of its users (the very thing it purported to avoid) to avert a potential miner collusion to form a 51% attack. The emergence of a multitude of new intermediaries seems to indicate that even with cryptocurrencies, banking and financial intermediaries may still have some usefulness as a layer of protection for consumers after all.

Fourth, we pointed out that Bitcoin's pseudo-anonymous payment system provided a very limited layer of protection for the privacy of user transactions. As with security, Bitcoin puts most of the burden of privacy protection on its users' shoulders, which creates a disparity in user privacy along the same lines as the digital divide in technology knowledge. Therefore, paradoxically, for the average user, Bitcoin might provide a lesser level of transaction privacy than traditional financial intermediaries. And even if Bitcoin did provide a better level of transaction privacy than conventional currencies, it would generate a range of further questions as to the possibility of law enforcement against crime and tax evasion.

Therefore, contrary to what its proponents might hope for, Bitcoin is far from fulfilling its promises to be a stable, efficient, radically decentralised and privacy-protecting currency. The reason for its relative popularity and substantial valuation lies thus either in unrealistic expectations from its users as to its capacity to act as a functioning currency, or in the prospects of rewards allowed by its status of high-risk speculative asset.

This, in turn, does not mean that cryptocurrencies are a useless development altogether. Their advent has brought about a great number of worthy innovations, with many useful applications. In particular, Bitcoin's distributed ledger technology might find useful applications in many areas. Some have hailed blockchain's potential in fostering decentralised organisation, by reducing the transaction costs of organising cooperation among a great number of individuals (de Filippi and Wright, 2018, p. 136). Even central and private banks have started looking into using blockchain technology, not so much for introducing cryptocurrencies (although such plans do exist [12]) but mainly to improve on their infrastructure for areas such as clearing and settlement or trade finance (Arnold, 2017). While these projects are clearly inspired by the technological innovations behind Bitcoin, they are likely to significantly diverge from Bitcoin's main ideological commitments (Bordo and Levin, 2017). Blockchain technology could also possibly be used in countries where banks cannot be trusted, or where the monetary system is failing, as some have argued (Varoufakis, 2014). In general, blockchain could be used to reduce costs (although on the condition of adopting alternative mechanisms to reduce its environmental impact) [13] and make payment settlements easier. However, with blockchain applications such as Bitcoin, it is important to take such claims with a grain of salt, and go beyond the overly enthusiastic rhetoric to assess the actual merits of the technology.

If its proponents want Bitcoin to become more than a speculative asset, they will probably have to adopt a more explicit and formalised governance to be able to seriously tackle not only mere technical challenges, but also the underlying political choices behind them as to the cryptocurrency's future. The question remains however, whether Bitcoin can be reformed so as to become a workable currency, while still retaining some of the attractiveness that its enthusiast saw in its initial promises. As of today, Bitcoin seems far from being the future of money.

REFERENCES

Aglietta, M., and Orléan, A. (2002). *La monnaie: entre violence et confiance*. Paris: Odile Jacob.

Ali, R., Barrdear, J., Clews, R. and Southgate, J. (2014a). Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin*, Q3. Retrieved from https://econpapers.repec.org/article/boeqbullt/0147.htm

Ali, R., Barrdear, J., Clews, R. and Southgate, J. (2014b). The economics of digital currencies. *Bank of England Quarterly Bulletin*, Q3. Retrieved from https://www.bankofengland.co.uk/-/media/boe/files/digital-currencies/the-economics-of-digital-currencies

Ametrano, F. M. (2016). *Hayek Money: The Cryptocurrency Price Stability Solution* (SSRN Scholarly Paper No. ID 2425270). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2425270

Angel, J. J., and McCabe, D. (2015). The Ethics of Payments: Paper, Plastic, or Bitcoin? *Journal of Business Ethics*. *132*(3), 603–11. doi:10.1007/s10551-014-2354-x

Arnold, M. (2017, October 16). Five ways banks are using blockchain. *Financial Times*. London.

Bershidsky, L. (2014, July 17). Trust Will Kill Bitcoin. *Bloomberg View*. Retrieved from http://www.bloombergview.com/articles/2014-07-17/trust-will-kill-Bitcoin

Bjerg, O. (2016). How is Bitcoin Money? *Theory, Culture and Society*, *33*(1), 53–72. doi:10.1177/0263276415619015

Blinder, A. S. (2010). How Central Should the Central Bank Be? *Journal of Economic Literature*, *48*(1), 123–133. doi:10.1257/jel.48.1.123

Böhme, R., Christin, N., Edelman, B. and Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *The Journal of Economic Perspectives*, *29*(2), 213–238. doi:10.1257/jep.29.2.213

Bordo, M. D. (2008). History of monetary policy. In S. N. Durlauf and L. E. Blume (Eds.), *The New Palgrave Dictionary of Economics* (second edition, pp. 715–721). Basingstoke: Palgrave MacMillan.

Bordo, M. D., and Levin, A. T. (2017). *Central Bank Digital Currency and the Future of Monetary Policy* (Working Paper No. 23711). Cambridge (Mass.): National Bureau of Economic Research. doi:10.3386/w23711

Bordo, M. D., and Schwartz, A. J. (1995). The Performance and Stability of Banking Systems under 'Self-Regulation': Theory and Evidence. *Cato Journal*, *14*(3), 453–479.

Cheah, E.-T. and Fry, J. (2015). Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. *Economics Letters*, *130*, 32–36. doi:10.1016/j.econlet.2015.02.029 Retrieved from https://eprints.soton.ac.uk/410439/

Collard, B. (2017, January 4). Le Bitcoin, la monnaie de la liberté. Retrieved 2 March 2018, from https://www.contrepoints.org/2017/01/04/276673-bitcoin-monnaie-de-liberte

Davis, J. (2011, October 10). The Crypto-Currency: Bitcoin and its mysterious inventor. *The New*

Yorker, New York. Retrieved from https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency

De Filippi, P., and Loveluck, B. (2016). The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure. *Internet Policy Review*, *5*(4). doi:10.14763/2016.3.427

De Filippi, P., and Wright, A. (2018) Blockchain and the Law. The Rule of Code. Cambridge, (Mass.): Harvard University Press.

Deetman, S. (2016, March 29). Bitcoin Could Consume as Much Electricity as Denmark by 2020. Retrieved from https://motherboard.vice.com/en_us/article/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020

de Laat, P.B. (2007). Governance of open source software: state of the art. *Journal of Management and Governance*, *11*(2), 165–177. doi:10.1007/s10997-007-9022-9

Dodd, N. (2017). The social life of Bitcoin. *Theory, Culture and Society*. Retrieved from doi:10.1177/0263276417746464

Dowd, K. (2014). *New Private Monies: A Bit-Part Player?* Hobart Paper 174. London: Institute of Economic Affairs.

Dwyer, G. P. (2015). The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, *17*, 81–91. doi:10.1016/j.jfs.2014.11.006

European Banking Authority. (2013). *Warning to consumers on virtual currencies* (Statement n° EBA/WRG/2013/01). Retrieved from https://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies

European Central Bank. (2012). Virtual Currency Schemes. Frankfurt am Main. Retrieved form www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf

European Central Bank. (2015). Virtual currency schemes: a further analysis. Frankfurt am Main. Retrieved from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

Friedman, M. (1959). *A Program for Monetary Stability*. New York: Fordham University Press.

Friedman, M. (1969). *The optimum quantity of money and other essays*. Chicago: Aldine.

Friedman, M., and Schwartz, A. J. (1963). *A monetary history of the United States 1867-1960*. Princeton, N.J: Princeton university press.

Frisby, D. (2014). *Bitcoin: The Future of Money?* London: Unbound

Gibbs, S. (2018, February 26). EU finance head: we will regulate bitcoin if risks are not tackled. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2018/feb/26/eu-finance-head-regulate-bitcoin-cryptocurrencies-risks

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C. and Siering, M. (2014). Bitcoin - Asset or Currency? Revealing Users' Hidden Intentions. *Proceedings of the 22nd European Conference on Information Systems*. Tel Aviv, Israel. Retrieved from

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425247

Golumbia, D. (2016). *The Politics of Bitcoin*. Minneapolis, MN: University of Minnesota Press.

Goodhart, C. A. E. (1991). Are central banks necessary? In F. Capie and G. E. Wood (Eds.), *Unregulated banking: chaos or order?* (pp. 1–21). London: MacMillan.

Goodhart, C. A. E. (2011). The changing role of central banks. *Financial History Review*, *18*(2), 135–154. doi:10.1017/S0968565011000096

Goodhart, C. A. E., Gabor, D., Vestergaard, J., and Ertürk, I. (2014). *Central Banking at a Crossroads: Europe and Beyond*. London: Anthem Press.

Goodin, D. (2014, June 15). Bitcoin security guarantee shattered by anonymous miner with 51% network power. Retrieved from http://arstechnica.com/security/2014/06/Bitcoin-security-guarantee-shattered-by-anonymous-miner-with-51-network-power/

Graeber, D. (2011). *Debt the first 5,000 years*. Brooklyn, N.Y.: Melville House.

Grinberg, R. (2011). Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science and Technology Law Journal*, *4*, 159–207.

Gruber, S. (2013). Trust, identity and disclosure- are Bitcoin exchanges the next virtual havens for money laundering and tax evasion? *Quinnipiac Law Review*, *32*(1), 135–208. Retrieved from https://papers.ssrn.com/abstract=2312110

Guadamuz A. & Marsden Ch. (2015) Blockchain and Bitcoin: Regulatory responses to cryptocurrencies, *First Monday*, *20*(12). Retrieved from https://firstmonday.org/article/view/6198/5163

Hajdarbegovic, N. (2014, January 9). Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack. *Coindesk.Com*. Retrieved from https://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack/

Hayek, F. A. von. (2007). *The Road to Serfdom: Text and Documents--The Definitive Edition*. (B. Caldwell, Ed.). Chicago: University Of Chicago Press. (Original work published 1944)

Hayek, F. A. von. (1990) [1976]. Denationalisation of money: the argument refined: an analysis of the theory and practice of concurrent currencies (3rd edition). London: Institute of Economic Affairs.

Hintz, A. (2014). Outsourcing Surveillance—Privatising Policy: Communications Regulation by Commercial Intermediaries. *Birkbeck Law Review*, *2*(2), 349. Available at http://orca.cf.ac.uk/70838/

Houy, Nicolas. (2014). The Economics of Bitcoin Transaction Fees. GATE Working Paper 2014/07. Retrieved from https://halshs.archives-ouvertes.fr/halshs-00951358

Ingham, G. (2004). *The Nature of Money*. Cambridge: Polity.

Kaminska, I (2017, September 18). What is 'Utility Settlement Coin' really? Financial Times Alphaville. London

Kaplanov, N. M. (2012). Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation. *Loyola Consumer Law Review*, *25*(1), 111–174. Retrieved from https://www.ssrn.com/abstract=2115203

Karlstrøm, H. (2014). Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: Scandinavian Journal of Social Theory*, *15*(1), 23–36. doi:10.1080/1600910X.2013.870083

Katz, L. (2017, July 19). Bitcoin Acceptance Among Retailers Is Low and Getting Lower, Bloomberg, https://www.bloomberg.com/news/articles/2017-07-12/bitcoin-acceptance-among-retailers-is-low-and-getting-lower

Kemp, R. (2010). Open source software (OSS) governance in the organisation. *Computer Law & Security Review*, *26*(3), 309–316. doi:10.1016/j.clsr.2010.01.008

Kindleberger, C. P. (1973), *The World in Depression, 1929-1939*. London: Allen Lane.

Kindleberger, C. P. (1978). *Manias, Panics, and Crashes: A History of Financial Crises*. New-York: Basic Books.

Kollewe, J. (2018, February 8). ECB official backs bitcoin clampdown. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2018/feb/08/ecb-official-backs-bitcoin-clampdown

Lakomski-Laguerre, O., and Desmedt, L. (2015). L'alternative monétaire Bitcoin□: une perspective institutionnaliste. *Revue de la régulation*, (18), 1–19. doi:10.4000/regulation.11593

Lee, T. B. (2018, February 20). Bitcoin's transaction fee crisis is over—for now. *Ars Technica*. Retrieved from https://arstechnica.com/tech-policy/2018/02/bitcoins-transaction-fee-crisis-is-over-for-now/

Lee, S., Baek, H., and Jahng, J. (2017). Governance strategies for open collaboration: Focusing on resource allocation in open source software development organizations. *International Journal of Information Management*, *37*(5), 431–437. doi: 10.1016/j.ijinfomgt.2017.05.006

Lehdonvirta, V. (2016). The blockchain paradox: Why distributed ledger technologies may do little to transform the economy. *Oxford Internet Institute*. Retrieved from https://www.oii.ox.ac.uk/blog/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/

Luu, J. and Imwinkelried, E. J. (2015). *The Challenge of Bitcoin Pseudo-Anonymity to Computer Forensics* (UC Davis Legal Studies Research Paper Series n° 462). Retrieved from https://papers.ssrn.com/abstract=2671921

Marian, O. Y. (2013). Are Cryptocurrencies 'Super' Tax Havens? *Michigan Law Review First Impression*, *112*(38). Retrieved from https://papers.ssrn.com/abstract=2305863

Maurer, B., Nelms, T. C., and Swartz, L. (2013). "When perhaps the real problem is money itself!": the practical materiality of Bitcoin. *Social Semiotics*, *23*(2), 261–277. doi:10.1080/10350330.2013.777594

McLeay, M., Radia, A. and Thomas, R. (2014). Money creation in the modern economy. *Bank of England Quarterly Bulletin*, Q1. Retrieved from https://www.bankofengland.co.uk/-

/media/boe/files/quarterly-bulletin/2014/money-creation-in-the-modern-economy

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M. et Savage, S. (2013). "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names", *Proceedings of the ACM SIGCOMM Internet Measurement Conference*, IMC, 2013, 127–139. doi:10.1145/2504730.2504747 Retrieved from https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

Mersch, Y. (2018). *Virtual or virtueless? The evolution of money in the digital age*. London: Official Monetary and Financial Institutions Forum. Retrieved from https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180208.en.html

Miers, I., Garman, C., Green, M., and Rubin, A. D. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin. Presented at the IEEE Symposium on Security & Privacy, Oakland. Retrieved from http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from http://www.Bitcoin.org/Bitcoin.pdf

Nakamoto, S. (2009). *Bitcoin open source implementation of P2P currency*. Retrieved from http://p2pfoundation.ning.com/forum/topics/Bitcoin-open-source

Nozick, R. (1974). *Anarchy, State and Utopia*, New York, Basic Books.

O'Mahony, S. and Ferraro, F. (2007). The emergence of Governance in an Open Source Community, *Academy of Management Journal*, *50*(5), 1079–1106. doi:10.2307/20159914 Retrieved from https://www.jstor.org/stable/20159914

Orcutt, M. (2017, September 11). Criminals Thought Bitcoin Was the Perfect Hiding Place, but They Thought Wrong. *MIT Technology Review*. Retrieved from Criminals Thought Bitcoin Was the Perfect Hiding Place, but They Thought Wrong

Popper, N. and Abrams, R. (2014, February 25). Apparent Theft at Mt. Gox Shakes Bitcoin World. *The New York Times*. New York. Retrieved from http://www.nytimes.com/2014/02/25/business/apparent-theft-at-mt-gox-shakes-Bitcoin-world.html

Redman, J. (2017a, May 6). The Bitcoin Network's Transaction Queue Breaks Another Record. Bitcoin.com, https://news.bitcoin.com/bitcoin-transaction-queue-breaks-record/

Redman, J. (2017b, June 9). Rising Network Fees Are Causing Changes Within the Bitcoin Economy. Bitcoin.com, https://news.bitcoin.com/fees-causing-changes-bitcoin-economy/

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

Rochard, P. (2013). *The Bitcoin Central Bank's Perfect Monetary Policy*. Satoshi Nakamoto Institute. Retrieved from https://nakamotoinstitute.org/mempool/the-bitcoin-central-banks-perfect-monetary-policy/

Rothbard, M. (2016). Essentials of Money and Inflation. In J. T. Salerno, M. McCaffrey (Eds.), *The Rothbard Reader* (157–162). Auburn, Alabama: Ludwig von Mises Institute. Available at

https://mises.org/library/rothbard-reader

Sedgwick, K. (2018, January 3). Bitcoin Fees Are Falling Amidst Greater Segwit Adoption. *Bitcoin.Com*. Retrieved from https://news.bitcoin.com/bitcoin-fees-are-falling-amidst-greater-segwit-adoption/

Tobin, J. (2008). Money. In S. F. Durlauf and L. E. Blume (Eds.), *New Palgrave Dictionary of Economics* (Second Edition). Basingstoke: Palgrave MacMillan. Retrieved from http://www.dictionaryofeconomics.com/article?id=pde2008_M000217

Torpey, K. (2018, January 31). Bitcoin Transaction Fees Are Pretty Low Right Now: Here's Why. *Bitcoin Magazine*. Retrieved from https://bitcoinmagazine.com/articles/bitcoin-transaction-fees-are-pretty-low-right-now-heres-why/

Urquhart, A. (2016). The inefficiency of Bitcoin. *Economics Letters*, *148*, 80-82. doi:10.1016/j.econlet.2016.09.019

Varoufakis, Y. (2014, February 15). Bitcoin: A flawed currency blueprint with a potentially useful application for the Eurozone. Retrieved from http://yanisvaroufakis.eu/2014/02/15/Bitcoin-a-flawed-currency-blueprint-with-a-potentially-useful-application-for-the-eurozone/

Vidan, G. and Lehdonvirta, V. (2018). Mine the Gap: Bitcoin and the Maintenance of Trustlessness. SSRN Scholarly Paper ID 3225236. Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=3225236.

Vigna, P. and Casey, M. J. (2015) The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order. New York:St. Martin's Press

Wallace, B. (2011, November 23). The Rise and Fall of Bitcoin. *Wired Magazine*. Retrieved from https://www.wired.com/2011/11/mf_Bitcoin/

Yermack, D. (2013). *Is Bitcoin a Real Currency? An economic appraisal* (Working Paper No. 19747). National Bureau of Economic Research. Retrieved from www.nber.org/papers/w19747

FOOTNOTES

1. See www.mapofcoins.com for a comprehensive list of existing cryptocurrencies and their underlying technologies.

2. While we will focus on Bitcoin, our discussion could also apply to other cryptocurrencies insofar as they share some of Bitcoin's characteristics and aims.

3. See Aglietta and Orléan (2002, 84–85), Tobin (2008, 1) and Graeber (2011, 46–47).

4. For a detailed presentation of how transactions in Bitcoins works, see Ali et al. (2014a, p. 7–8). For an overview of bitcoin, see Böhme et al. (2015).

5. In that regard, let us note the inclusion of virtual currency exchanges and "custodian wallet services" among the services regulated by the recently adopted 5th Anti-Money Laundering Directive, Directive 2018/843. In the US, although no new legislation was adopted on the matter, these services are effectively considered as covered under the Bank Secrecy Act according FinCEN's guidance on virtual currencies, US Department of Treasury, 18 March 2013.

6. As described on the website of the Belgian Ministry of Finance: http://fondsdegarantie.belgium.be/fr

7. These statistics are based on our own computations, thanks to data collected on blockchain.com. See also Lee (2018).

8. According to statistics from blockchain.com.

9. US Department of Treasury, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, 18 March 2013.

10. Directive 2018/843 of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, art. 1.

11. See Miers et al (2013)

12. UBS and a consortium of financial institutions are reportedly developing a central bank backed cryptocurrency called Utility Settlement Coin, on which few details are known (Kaminska 2017)

13. Indeed, although Bitcoin's proof-of-work security algorithm has been rightly criticized for its high environmental impact (see Deetman, 2016), alternative security algorithm that are less energy intensive have been proposed (such as "proof-of-stake" algorithm, which would rely less on solving difficult computational problems, by replacing "computational power" with "financial stake" as a consensus mechanism)