JOURNAL OF PEER PRODUCTION
Journal of Peer Production
ISSN: 2213-5316
http://peerproduction.net

The Paradoxes of Distributed Trust: Peer-to-Peer Architecture and User Confidence in Bitcoin

Alexandre Mallard, Cécile Méadel and Francesca Musiani

Abstract:

The decentralized electronic currency system Bitcoin gives the possibility to execute transactions via direct communication between users, without the need to resort to third parties entrusted with legitimizing the concerned monetary value. In its current state of development - a recent, fast-changing, volatile and highly mediatized technology - the discourses that unfold within spaces of information and discussion related to Bitcoin can be analysed in light of their ability to produce at once the representations of value, the practices according to which it is transformed and evolves, and the devices allowing for its implementation. The literature on the system is a testament to how the Bitcoin debates do not merely spread, communicate and diffuse representation of this currency, but are closely intertwined with the practice of the money itself. By focusing its attention on a specific corpus, that of expert discourse, the article shows how, introducing and discussing a specific device, dynamic or operation as being in some way related to trust, this expert knowledge contributes to the very definition and shaping of this trust within the Bitcoin system - ultimately contributing to perform the shared definition of its value as a currency.

Keywords: Bitcoin, decentralization, currency, trust, peer-to-peer, expert discourse, value, devices, money

Alexandre Mallard, Cécile Méadel and Francesca Musiani

Introduction

The construction of new forms of electronic currency is one of the application fields of peer-to-peer (P2P) technology that has led to a number of innovative developments in recent years.(i) Bitcoin is certainly among the most interesting examples in this regard. Based on a P2P protocol published in 2009 by a mysterious developer or group of developers (Nakamoto, 2009), and quickly adopted by Internet users, this currency has developed steadfastly to the point that it has already experienced several downfalls (Wallace, 2011). The number of Bitcoin transactions is now estimated at 40,000 each day, and its volume of transactions is believed to have reached $1 billion.(ii) As is often the case in the P2P universe innovators aim at offering alternatives to existing services, as the core features of distributed network architectures offer both the possibility of new technical features and the opportunity to promote different socio-political principles in the daily practice of Internet-based services. One of the standout features of Bitcoin is the promise of 'doing without' intermediaries such as banks, financial institutions or political authorities dedicated to monetary exchange and regulation. All of these intermediaries are accused of (expensively) alienating currency and leaving what is understood as a 'common good' to a capitalism that has been confronted with new challenges stemming from the 2007-08 global economic crisis. Doing without intermediaries would imply getting rid of the institutional guarantors of monetary trust, i.e. the recognition of a medium of payment to be valid for meeting a financial obligation, by all parties within a legal system. The functioning of 'official' currency relies upon the existence of actors such as central banks, the ultimate guarantors of the value of the circulating goods and titles. Inversely, Bitcoin offers the possibility to execute transactions via direct communication between users, without the need to resort to third parties entrusted with legitimizing the concerned monetary value. Thus, it appears to emphasize, and perhaps give new meaning to, the centrality of the social nature of monetary exchange – an argument that is at the core of the work of scholars such as David Graeber (2011), Geoffrey Ingham (1996) and Viviana Zelizer (1997). Furthermore, it provides a field of unprecedented interest for the observation of the 'political economy of peer production', the new production, governance and property dynamics emerging as a result of the progressive transformation of the complex systems surrounding our daily lives into distributed networks (Bauwens, 2005). Bitcoin challenges the notion of trust bonded to a central bank with the guarantees of a distributed trust, specific to technologies based on a peer-to-peer architecture. This ambition – and the debates and controversies it raises – constitute the focus of this article.

Our approach is situated within a body of work in the sociology of innovation, conducted recently on the topic of P2P technology applied to Internet services (Musiani, 2013) and grounded in actor-network theory (Akrich, Callon & Latour, 2006; Callon, Méadel & Rabeharisoa, 2002; Callon et al., 2013). We will consider the socio-economic development of the Bitcoin system as that of a monetary innovation, whose functioning requires not only the implementation of novel technical arrangements, but also the emergence of new forms of cooperation and the construction of shared meanings among the actors involved in its use. This is frequently observed in innovation processes; in the case of money, these forms of cooperation and shared meanings intersect the question of value. The starting point of our reflections is the idea that currency can be understood by means of the link it builds between the devices involved in its use, and the conceptions of the value it embodies. This especially applies to operations such as payment, transfers, and the measurement or the preservation of value, which are the main functions traditionally identified by economists and anthropologists exploring the construction of value as it relates to monetary systems (Maurer, 2006; Blanc, 2009).(iii) In this perspective, the question of trust and confidence relates to the modality of establishing a heterogeneous network involving various monetary devices and human actors, and endowed with the capacity to enact the circulation of value. To suggest that the use of P2P software allows for a monetary translation – in the sense Callon (1986) uses this term – that is trustworthy, is equal to suggest that stakeholders in this transaction recognize clearly the transformations in value that are associated with this use. In line with this approach, this article does not provide an a priori definition of trust, beyond a very basic understanding of it as reliance on another person or entity. Instead, we will observe trust taking shape through interactions between actors and technologies, transactions, discourses and debates, in several arenas ranging from governance to social interaction and technology implementation. Definitions of trust are meant to take shape ex-post, out of both the analysis and the narrative.

Thus, the way in which we propose to analyse the question of trust in P2P currency is to examine the construction of the links between the technical devices specific to Bitcoin and the monetary significances and meanings

they entail. In an overwhelming majority of cases, the history of innovation has shown that innovation processes are accompanied by a number of discussions, debates, and controversies, by means of which the relations between technology, practices and meanings are gradually negotiated. The 'stabilisation' of the innovation usually happens with the establishment of a configuration in which the technical devices and infrastructures become transparent or invisible (Akrich et al., 2006). The analyst who becomes interested in this dynamic appears to have nothing but fieldwork choices and opportunities in the specific case of Bitcoin: even a short Internet search is sufficient to assess today's impressive proliferation of discourses aiming at explaining the functioning of Bitcoin, accounting for the trustworthiness of the transactions that this system makes possible, and debating its 'truly monetary' qualities (volatility, liquidity, stability). Innumerable discourses of this variety are found in blogs, wikis, forums, information sites, exchange platforms, online (or even offline) information magazines, discussion websites specialized in economy, finance, computer science (including a fully dedicated one (iv)), and so on.(v) These discourses include a wide-ranging palette of topics related to the extent of participation and the degree of competence of actors in the Bitcoin universe. They include introductory 'guidebooks' for curious newcomers to a currency qualified as revolutionary, information for dedicated amateurs of e-commerce seeking 'good business' in eBay style, or yet again, financial, real-time information for companies or professional traders who have already been experimenting with the system for years and are trying to understand how its outputs could become market assets.

Our research-in-progress on Bitcoin has led us to conduct different investigations on these spaces of information and discussion. Nonetheless, we wish to differentiate our analytical approach from the perspective that sees the discourses observed within these spaces as social representations fuelling the constitution of 'monetary beliefs' (i.e., the collective 'power of multitudes' that, believing in the legitimacy of money, supports it as a system, with the same degree of effectiveness held by juridical guarantees; Orléan, 2007). The notion of monetary belief plays an important role in a number of analyses dedicated to money and currency – be it in the approaches informed by economics that explore how this notion supports self-fulfilling prophecies, or the perspectives influenced by sociological thought that address belief as the logic underpinning the influence of social forces on economic actors (notably inspired by Emile Durkheim, from Simiand, 1934 to Orléan, 2009). Inversely, it seems to us that these discussion spaces can be understood as 'hybrid forums' in which a variety of actors debate the organization of today's economy and the qualities of the goods circulating within it (Callon et al., 2002 and 2013). Thus, the discourses that unfold within these spaces can be analysed in light of their performative nature (Callon, 2007), that is, their ability to produce at once the representations of value, the practices according to which it is transformed and evolves, and the devices allowing for its implementation. This perspective seems almost 'natural' to adopt in Bitcoin's current state of development: the electronic literature on the system is a witness to how the Bitcoin debates do not merely spread, communicate and diffuse representation of this currency, but are closely intertwined with the practice of the money itself. The most emblematic case is the variety of Bitcoin-related forums, where users go to look for information vital to their very understanding and use of the system.

Within the frame of this article we focus our attention on a specific corpus, that of expert discourse – experts belonging to different technical disciplines interested in the development of this currency: software engineering, cryptography, economy, communication, law, and economic anthropology. In the same manner as the discussion forums, the literature of technical experts concerning Bitcoin is currently proliferating. Interestingly, most of this literature is not clearly falling into the category of scientific article, nor of generalist press. Instread, most contributions are 'hybrids', such as Satoshi Nakamoto's pioneering article, which established Bitcoin's initial framing and definition. This is most likely due to the novelty of the system , the complexity and rapid evolutions of its underlying mechanism, based on a non-hybrid 'radical' version of P2P, and on elaborate cryptographic mechanisms. Still, there are several embryos of academic literature that is concerned with the economic, social and legal implications of Bitcoin (and often, more generally, of distributed electronic currency).

A first analysis of scientific databases returned a relatively unsuccessful result(vi); however, subsequent attempts with a hybrid search engine such as the deceased Scirus(vii) proved far more successful, by returning several hundred references, including scientific journals as well as researcher blogs, conference websites, and research collectives. These works adopt a number of different perspectives on Bitcoin, more or less cognate to our analysis – the most compatible one being the article authored by Bill Maurer et al. (2013). We undertook a qualitative analysis of thirteen of these documents, authored by researchers (often also practitioners) representative of different disciplines (Androulaki et al., 2012; Brezo & Bringas, 2012; Corcoran, 2013; Elias, 2011; Grinberg, 2011; Jacobs, 2011; Jansen, 2012; Kaplanov, 2012; Maurer et al., 2013; Mendoza, 2012, 2013; Noizat, 2012; Wallace, 2011). These articles allowed us to complete an exploratory mapping of the different issues that are considered by experts as being associated with the emergence of a 'distributed trust' in Bitcoin. We hypothesize that, by introducing a specific device, dynamic or operation as being in some way related to trust, this expert knowledge contributes to the very definition and shaping of this trust within the Bitcoin system – ultimately contributing to the shared definition of its value as a currency.

The rest of this article is organized as follows. After briefly introducing Bitcoin's main functioning principles, we will examine four dimensions of the debates related to the implementations of distributed trust delineated or proposed by this system – dimensions that correspond, indeed, to quite different definitions of what constitutes trust in the first place. The first dimension addresses the connection between commodity money and credit money: Bitcoin-related discussions merge into a controversy that money historians and anthropologists are well acquainted with: the alternative between a conception of trust built upon the relation to objects and one built on the relation to social institutions. We will see how the tensions between these two declinations of trust, in the case of Bitcoin, are related to the decentralization of trust. The second dimension entails the ways in which trust in digital networks, more generally, influence the debate on monetary trust, more specifically. This point is especially relevant in the case of P2P networks, which raise in specific ways the question of resource pooling and allocation within the network, and thus, of the relationship between trust and the implementation of a functioning technical infrastructure. The third dimension addresses anonymity and transparency in the building of trust. An interesting feature of Bitcoin is its proposal of a combination of anonymity and transparency that reflects in often-unexpected ways on the associated trust features. Finally, the fourth dimension addresses the integration of Bitcoin into pre-existing monetary and economic systems, and how this influences or may influence trust-related debates. Bitcoin debates intersect here with classical questions in monetary analysis, such as the link between money volatility and the trust it elicits, or the governance arrangements for money and currency and their link with money credibility in diverse economic contexts.

Bitcoin: decentralized architecture for distributed trust?

One of Bitcoin's characteristics is the complexity of its functioning, which has little to compare with the functioning of currency as we traditionally understand and use it. We will introduce and discuss a number of Bticoin's functional elements throughout the article, and here we address only those elements necessary to the understanding of the system as a whole.

As a service operating on top of a peer-to-peer network, Bitcoin allows users to execute payments by digitally signing their transactions. It prevents the possible problem of double-spending 'digital' coins through a distributed time-stamping service. Users willing to undertake Bitcoin transactions need to install P2P software on their computer, which allows

them to issue and receive monetary units.(viii) The software allows users to generate electronic addresses in the form of encrypted keys that only the user can authenticate. These addresses further work as accounts in which Bitcoin goods may be stored. A transaction consists in sending into the network a predetermined amount from one address to the other. Each transaction between two users is collected in aggregated form in a 'block', which is itself integrated to a chain, the 'block chain'. According to a model common in P2P architecture, the block chain is not stored somewhere in a centralized way but it circulates, and is constantly shared, among all the members of the network. Thus, the block chain functions as a public repository including the history of all the transactions concluded after the currency system was launched, and thus enables one to know at any moment what is the repartition of goods among the different addresses active in the network. In order to guarantee the reliability of this information, only blocks pertaining to authenticated transactions may be added to the block chain. Thus, every block is subject to a verification that, in a nutshell, consists in examining every transaction in order to make sure – by comparing it with prior transactions – that users are actually in possession of the goods they wish to exchange. This verification process is carried out by some of the computers connected to the network. The Bitcoin software installed on the computers of every member of this monetary community aims at following the permanent flux of transactions, but it also allows, if users agree to it, to contribute to the computational power required for the verification of the block chain. Ultimately, this is a contribution to the authentication of the overall public repository. In exchange for this contribution, the user is rewarded by a given quantity of Bitcoins. Thus, it is through contributing to the authentication of the transactions, called mining, that monetary creation is enacted. Finally, we need to underscore a recurring element in Bitcoin debates: the technical protocol has been conceived in such a way that the quantity of money that is gradually 'freed' by the mining process, and corresponding to the monetary mass available for exchange, cannot exceed a predetermined amount of 21 million Bitcoins.

Bitcoin is not backed by any government or other legal entity, and not redeemable for gold or other commodity by such bodies. Its decentralized and distributed architecture does not imply any central entity in charge of regulating either the value or the amount of the total number of existing coins. These functions are delegated to the user network itself. The fact that the verification of transactions and the creation of money are implemented not by trusted third parties (e.g. banks) but by a distributed network of innumerable mining machines allows us to speak of the implementation of a distributed trust: every user that accepts to mine contributes a brick to the collective building of a trust that would, then, no longer need to be incarnated in specific institutional authorities.

1. Commodity money and credit money

As all sorts of actors have repeatedly mentioned (and evidenced by the frequent use of the term 'revolution', e.g. Salyer, 2013) the functioning of this P2P money does not resemble, at a first glance, anything known before in this field. The astonishment and the difficulty we experience when attempting to understand in detail the ways that value is produced, circulated and preserved in this network are certainly comparable, in principle, to previous transitions from one monetary paradigm to the other. One of the great transformations in the field of monetary technology that is frequently recalled in Bitcoin-related literature is the shift from a system where currency as a material device has an intrinsic value, that of a specific product, a precious metal (commodity money), to a system where the intrinsic value is no longer present and currency is, in fact, a series of mutually accepted debts (credit money). David Graeber refers to this dynamic as a shift from evaluating things to evaluating actions (Graeber, 2001: 49). It seems that we cannot clearly position Bitcoin vis-à-vis one or the other of these alternatives.

Bitcoin's project explicitly attempts to break with credit money models that suppose the existence of a chain of intermediaries, guarantors of trust, originating from a central authority that has the right to act as the ultimate lender. The political discourse of Bitcoin is indeed born against this type of social organization. Yet, the label used to indicate the procedure of monetary creation (the mining), and the very idea of a mandatory, finite quantity of existing currency, has analogies with the intrinsic-value, precious-metal model used in several civilizations as the foundation of monetary value. Maurer et al. (2013) use the notion of 'digital metallism' to render the surprising combination of materiality and virtuality that characterizes Bitcoin. This term underlines Bitcoin's dematerialization in which the value is incarnated such as commodity money is in gold, and also the fact that, as with every technology supported by digital networks, the dematerialization of money itself is accompanied by the implementation of heavy material infrastructure.

However, in other respects Bitcoin seems to resemble credit money. Elias (2011) acknowledges the difficulty of establishing the intrinsic value of Bitcoins and argues that Bitcoins are better compared, in some respects, to a fiduciary gold-standard based system or to a community system based on the trust of all members:

> While popular sentiment tends to treat Bitcoin as a type of commodity, Bitcoin also shares some characteristics with that of fiat money. At least one noted economist has described Bitcoin as a "private gold standard", because the quantity of Bitcoins which will ever come into existence is fixed, and the rate at which they are to be produced is known (although this quality is unique to Bitcoin, as new discoveries can occur in even the scarcest commodities). Whether or not Bitcoin has intrinsic value or not is unclear. Although one of the more promising uses of Bitcoin which would instill intrinsic value is that of triple entry accounting. Likely to be some amalgamation of the aforementioned systems, it is certain that Bitcoin is "an agreement amongst a community of people to use 21 million secure mathematical tokens". (Elias, 2011)

Maurer et al. (2013) propose a radical interpretation of this ambiguity between commodity money and credit money, and define it as 'dialectic' at the very heart of Bitcoin. Their analysis reminds us that the opposition between these two monetary paradigms should not be juxtaposed a-critically on the opposition between technology and society. Reaching this conclusion would be like considering that one of the systems inscribes value in objects, while the other inscribes it in social institutions. Trust would, in the first case, be located in the relationship of the subject to the object, and in the second case, in the relationship of the subject to his or her ruler. With a precious metal or with a political authority, trust would nonetheless be centralized.

Maurer et al.'s analysis invites us to reconsider this juxtaposition of dualisms and to recognize that, in both cases, the reliability of the money is based on a trust that is shared among individuals and supported by multiple institutions and technical infrastructures, producing specific outputs that must be examined each time. Indeed, the history of the emergence of credit money shows that the birth of the system that has guaranteed its reliability cannot be read purely and simply as the installation of social authorities centralizing a capital of trust. The transformation of the forms taken by trust happens in the shift from a situation where credit was already widespread, but relying on the support of technical devices (as the bills of exchange did not allow to compute reputation) to a situation where debt becomes inscribed in repositories making them computable. In addition, Maurer et al., recalling Ingham's analyses (2004, 1996), underscore that money's function as a system supposed far more complex social processes than the mere inscription of trust in a precious metal.

If applied to the Bitcoin case, these analyses suggest that the notion of trust in the code, which is at the heart of the functioning of this P2P money, should not be taken literally:

> Insofar as Bitcoin's promises – of materiality, privacy, and community – are the stuff of credit, as we suggest below, Bitcoin provides a useful reflection on the sociality of money, despite its embedding of that sociality of trust in its code itself. In this world, there is no final settlement – as with a state demanding payment in the form of taxes or tribute – and trust in the code substitutes for the (socially and politically constituted) credibility of persons, institutions, and governments. It is this – not the anonymity or the cryptography or the economics – that makes Bitcoin novel in the long conversation about the nature of money. (Maurer et al., 2013)

These reflections allow for a first conclusion on the use of the notion of trust in Bitcoin. 'Trust in the code' entails a high degree of ambivalence. It calls for the necessity of examining in a more detailed way how forms of trust are de facto engaged and embedded in the manipulation of the technical devices in the Bitcoin system. This is the subject of the following sections.

2. Trust in digital networks, trust in money

As recent work on decentralized network architectures applied to Internet services has shown (Aigrain, 2010; Moglen, 2010; Musiani, 2013), specific balances of competences and responsibilities between service providers, content producers, users and network operators take shape in decentralized services. New forms of interaction between the local and the global suggest, in turn, the rise of innovative ways to do 'politics by other means' (Latour, 1988: 229), to articulate the individual and the collective. The diverse forms of engagement and intéressement (Callon, 1986) – of pioneer users first and foremost, but also of other actors involved with the implementation and the operations of the services – contribute to the shaping of innovative ways to address classical questions in sociology of innovation. These include the sustainability of the underlying economic models, the technical and legal approaches to digital content and personal data, and last but not least, the building of reputation, confidence and trust in the system and in other users.

Within this scenario, Bitcoin shows its own peculiar interweaving of different dimensions of trust. On the one hand, these are related to trust in digital networks and on the other, to monetary trust. The issue of user trust in digital networks is often worked on by computer, software and network engineers, yet they raise the question in a different way to how economists consider trust in money. More specifically, the building of trust in Bitcoin is closely connected with the fact that the digital network subtending it is a P2P network, which should be underlined alongside Maurer et al.'s arguments on trust in code and on the re-materialisation of money. P2P code, and the ways in which it 'distributes' interactions, engage specific forms of trust.

Delving into the founding elements of users' trust in a distributed networked system is often neglected by money analysts, who tend to give priority to the fiduciary entity and not to the technical arrangement or device that supports it. However, Bitcoin's P2P architecture engages specific forms of trust inasmuch as it redistributes responsibilities. Three aspects, in particular, engage trust and transform it and we will consider them in turn for the remainder of this section. The first is collective engagement: users must accept a system whose work is based on sharing and pooling individual resources. This entails an explicit act of joining the system, and an explicit participation in it as a result. This participation allows for the duplication of 'property rights' and aims at preserving the system as a 'repository of value'. The second element is technical complexity, which is both a guarantor and a potential weakness. A complex, resilient technical infrastructure, allowing for alternative routes – i.e., resilient because of its decentralization – can elicit trust. However, and for the same reasons, it can also be a source of problems, speculations, controversies, inaccurate word-of-mouth, inappropriate behaviour and misuses. The third aspect is the collective, yet partly differentiated, elaboration of both code and 'content' in the system. Users' roles, levels of engagement and types of intervention in the system differ, and those discontinuities – between those who co-develop the code and those who don't, between those who mine and those who 'limit themselves' to transactions – have structuring effects on Bitcoin's distributed trust.

Collective engagement in a 'repository of value'

Users' trust is first engaged in the connection to the rest of the P2P network and the acceptance of the sharing and pooling of a part of their computational resources with other users in the network. Indeed, the Bitcoin network leverages the computational capacity of its own users to manage and maintain itself, and in particular, the single and comprehensive record of all transactions that is crucial to its functioning. This is hardly a Bitcoin use-specific feature: as with other decentralized systems that we have analyzed recently, from search engines to storage platforms (Musiani, 2013), Bitcoin needs the 'work' and resources of users. This collective pooling of resources is the necessary infrastructure to support not only the record of the past, but the correct and reliable implementation of the system's functioning in the future:

> It is the network itself, making use of the computational capacity of its own users, the one that manages and maintains it. This calculation capacity is used, amongst other things, to manage the transaction history —what is known as the block chain— and to confirm and validate each and every new transactions (sic) to be happening in the future. (Brezo & Bringas, 2012)

The extent to which users can have trust in the Bitcoin P2P system as the embodiment of a 'repository of value' seems problematic. The problem of distrust in the computing system seems to appear when the question is raised of how value can be extracted and preserved somewhere, without fear of its disappearance. At stake in this case is not only the reliability of the technical system in general, but more specifically, the idea that a P2P network may lend itself poorly (or at least, ambiguously) to a role of 'repository of value'. This repository function is traditionally a central function of money. If in computing/networking terms the location of the 'Bitcoin wallet' is unclear, the repository function is under threat. However, it is counter-argued that the repository is, in fact, constituted by the block chain. Thus it is very much present and it can be 'located', even if it is widely distributed and duplicated. In this case, a much more important distrust factor than P2P as value repository is considered to be the high volatility and fluctuations of Bitcoin as a currency.

Unsurprisingly, the 'materiality' of the computational and storage resources needed to handle Bitcoins – and that of Bitcoins themselves – becomes an increasingly critical factor as the perceived value of Bitcoin increases. P2P clients and user equipment being the center of operations, they become the main point of vulnerability for the security of the system:

> Both the code and the idea of bitcoin may have been impregnable, but bitcoins themselves—unique strings of numbers that constitute units of the currency—are discrete pieces of information that have to be stored somewhere. By default, bitcoin kept users' currency in a digital "wallet" on their desktop, and when bitcoins were worth very little, easy to mine, and possessed only by techies, that was sufficient. But once they started to become valuable, a PC felt inadequate. Some users protected their bitcoins by creating multiple backups, encrypting and storing them on thumb drives, on forensically scrubbed virgin computers without Internet connections, in the cloud, and on printouts stored in safe-deposit boxes. But even some sophisticated early adopters had trouble keeping their bitcoins safe. (Wallace, 2011)

P2P technical complexity as guarantee and weakness

The decentralized architecture of the system is at once what can act as a guarantor against attacks and errors (because of the resilience it provides) but can also become a source of problems, uncertainty, inaccurate word-of-mouth and circulation of incorrect information. Both of these tendencies are clearly revealed by the high number of papers dedicated to the dangers and pitfalls of Bitcoin's algorithm, and the practice and circulation of Bitcoin's software.

Moreover, the high threshold of initial investment necessary to understand how the system works, and to its correct use – that we are experiencing ourselves as newcomer scholars of the system – makes the Bitcoin technology an environment that is especially prone to activities of détournement and deviant behavior. Perception of anonymity is an example of this:

> The intrinsic complexity of the protocol and the necessity of having some relatively advanced knowledge on cryptography and computer studies to understand its real behaviour, make these cryptocurrencies the perfect place for speculation and misinformation. For instance, as already stated, there is a widespread belief of the mere fact of using it is sufficient guarantee to perform anonymous transactions, when this is not true by definition. (Brezo & Bringas, 2012)

A collective, yet differentiated, elaboration

As Maurer et al. (2013) underline, a 'sociality of code' takes place in Bitcoin. Both code and content in the system undergo a continuing elaboration process that is collective and yet partly differentiated among specific groups of users and machines. Users' roles, levels of engagement and types of intervention in the system differ, and those discontinuities have structuring effects on Bitcoin's distributed trust.

Mechanisms of trust are technology-based, embedded, and very much dependent on developers' design choices. As such, it is complicated for the 'lay' participant to fully understand who can modify and adapt the code, how they legitimize themselves, and even who they actually are – an issue epitomized by 'Satoshi Nakamoto''s dubious status. The question of intervention in the code remains opaque for users, and authors go as far as describing ongoing participation in the system as an act of faith:

> (Trust is) established through cryptographic proof via Bitcoin's network politics involving the rule of 'one-CPU-one-vote' and essentially depending on 'honest' nodes that obey the rules. When users adopt Bitcoin they put their faith in its code and the team of six developers, 'buying in' to its protocol including the embedded values that come along with it. (Jansen, 2012)

Moreover, the co-production of Bitcoins takes place at the cost of a differentiation or discontinuity between two groups: the miners and the 'others'. Trust-building means providing technical incentives for users and their equipment to act for the good of the system as a whole, in addition to their individual good – rather than in a manner that would be unsustainable for the network. Thus, the block chain: transactions are broadcasted in the Bitcoin network in a single, comprehensive and constantly updated register, and are subject to validity checks by the machines of other users in the system. As it frequently happens in decentralized systems, however, some peers are more important than others for the maintenance of the network: in Bitcoin's case, it's the miners. Miners add transaction records to Bitcoin's public register of past transactions, called the block chain, which serves to confirm to the rest of the network that a transaction has legitimately taken place. Block chains are meant to prevent double spending. While mining is intentionally designed to be resource-intensive and difficult, so that the number of blocks found each day by miners remains steady, a miner is granted 25 new BTCs every time a block is generated successfully, and this provides an incentive for miners to maintain their ongoing support of Bitcoin. The block chain process, which is assured by the resources and the relative stability of the nodes/miners, is a source of trust for the network in its entirety:

> [Each] resulting block is forwarded to all users in the network, who can then check its correctness by verifying the hash computation. If the block is deemed to be "valid", then the users append it to their previously accepted blocks, thus growing the Bitcoin block chain. Bitcoin relies on this mechanism to resist double-spending attacks; for malicious users to double-spend a BTC without being detected, they would not only have to redo all the work required to compute the block where that BTC was spent, but also they need to recompute all the subsequent blocks in the chain. (Androulaki et al., 2012)

Ultimately, issues of control on and with technology – its complexity, its intentional or unintentional opaqueness – are at the core of user adoption and trust in Bitcoin. On one hand, confidence may collapse because of technology- and code-related issues such as compromised anonymity, loss or theft of Bitcoins, or institutional/individual hacking into the system that would prevent transactions from settling (Grinberg, 2011). On the other hand, and despite the stated desire of Bitcoin's creators to remove or minimize the importance of trust issues, the importance to establish and stabilize trust in alternative ways, closely tied to the P2P nature of the system – collective engagement in resource pooling, resilience of decentralized networking technology – is strongly reaffirmed.

3. Anonymity, transparency, privacy and trust

The link between the building of trust in Bitcoin and questions related to the protection of personal information, such as anonymity, privacy and transparency, is a third important issue. Indeed, an interesting feature of Bitcoin is its proposal to combine anonymity and transparency, which reflects in oft-unexpected ways on the associated trust features (see also Maurer et al., 2013). We wish to focus especially on three issues: 1) the three dimensions of anonymity: cryptography, the verification of 'blocks' in the block chain, and the registration of transactions; 2) the paradox of hypothetically reintroducing 'privacy intermediaries' to address the publicity of the block chain; and 3) the link between users' technical skills and the degree of anonymity they can manage to preserve in the system.

Three-faced anonymity

The type of trust required by the link between 'transaction partners' in Bitcoin is shaped by the cryptography techniques subtending the system. Bitcoin as a system 'displays' to users its ability to create a link between two participants that is both reliable and anonymous: one node does not know who the other is, but is sure that it holds the value it transmits.

The functioning of Bitcoin essentially relies on three aspects: the robustness of cryptographic techniques, the ongoing verifications of the new Bitcoin blocks created and inserted in the system, and the registration of each transaction, which must be unique and comprehensive across all computers of the system. These three aspects are all carried out in a

decentralized manner by the machines of the users. Combined, they perform an equivalent function to that of a third party guarantor in other instances:

> Traditionally, a medium of exchange possessing any one of these characteristics meant that a trust based system was being utilized, in that a third party would need to be "trusted" in order to bring about one or more of these qualities. Bitcoin accomplishes these feats though the use of cryptography, and a single comprehensive record of all transactions. (Elias, 2011)

Reintroducing 'privacy intermediaries'?

The public nature of the transaction list, however, can raise issues. In the words of some authors, we arrive at the paradox of needing to add intermediaries to the system so as to ensure the privacy of actors, which goes against the social disintermediation of Bitcoin.

Bitcoin addresses – the virtual pseudonyms that identify users vis-à-vis the system – are the arrangement to which privacy protection for participants in the system is delegated. Each user possesses one or more Bitcoin addresses that are stored and managed by its P2P client, its digital wallet. Each address is linked to a unique public/private key pair: as other distributed systems that we have analyzed in the past, Bitcoin uses public-key cryptography, in which each user has a pair of cryptographic keys: a public encryption key and a private decryption key. The publicly available encrypting-key is widely distributed, while the private decrypting key is known only to its proprietor. The keys are related mathematically, but the parameters are chosen so that calculating the private key from the public key is either impossible or prohibitively expensive. In Bitcoin, these keys are used to authorize the transfer of the ownership of Bitcoins among addresses.

Thus, in the Bitcoin system, a privacy-by-design or privacy-by-architecture mechanism supersedes the need for a document outlining a privacy policy, which is a natural consequence of the absence of a service provider to whom the implementation and enforcement of the policy could be delegated. However, it is argued that users may have good reasons for considering that such a technique-embedded arrangement may be neither sufficient nor adequate to protect their privacy. This is because, in spite of the reliance on pseudonyms (supported and 'stabilized' by public-key cryptography), another necessary condition for the system's stability is the presence, continuous update, and public availability of the comprehensive transaction list (the block chain), through which the expenditure of individual coins can be publicly tracked. Interestingly, this may lead developers for whom privacy protection would be the prevalent concern to opt for an increased reliance on third-party entities. Considering that decentralization is one of the cornerstones of Bitcoin, this may raise serious trust issues among users:

> One possible technique to enhance privacy in Bitcoin would be therefore to require that vendors use a newly generated recipient address in each transaction that they receive; this address should be communicated to clients using a private channel […] the reliance on third-party trusted entities […] emerges as one of the few workable solutions to increase the privacy of Bitcoin clients. By storing the coins of a large number of users, these entities can hide the direct relationship between the inputs and outputs of a transaction within a sufficiently large anonymity set—and therefore better support the privacy of users. Clearly, this solution comes at odds with the main intuition behind Bitcoin, originally planned as a completely decentralized digital payment system [… however,] current measures adopted by Bitcoin are not enough to protect the privacy of users if Bitcoin were to be used as a digital currency in realistic settings. (Androulaki et al., 2012)

Better skills, better anonymity?

Some authors underline a possible correlation between users' technical skills and the degree of anonymity they can manage to preserve in the system. According to legal scholar Matthew Elias, the user's trust in his or her capacity to remain anonymous within the Bitcoin system is also linked to his or her perception of peer-to-peer networking and cryptography as anonymous technologies. However, it is also a function of one's technical knowledge and ability and of the amount of resources, both human and technical, that one is able to dedicate towards that end. It is, again, a matter of the priorities that developers embed in the system's design. It also provides users with tools to cope with complexity and control the consequences of their actions within the system:

> Bitcoin is anonymous to the extent that it is a digital, cash-like medium, which can be made to become more anonymous based on the technical knowledge and ability of an individual, and the resources at an individual's disposal. Bitcoin is a product of the internet, and therefore bears an intimate relationship to level of anonymity one is able to obtain therein. (Elias, 2011)

4. The (political) re-location of Bitcoin. From disintermediation to re-intermediation

The Bitcoin project builds upon a negative appreciation of the role of the intermediaries in the financial world(ix), who would be benefitting of unjust enrichment(x). Bitcoin aims at 'monetary liberty', and was initially set up under the assumption that transactions are not reported to banks or other intermediaries, but to those who allow the money to function (miners). Similarly, Bitcoin is developed within the frame of distrust in political authorities, i.e. States attempting to forbid specific transactions.

> Bitcoin is like Light and Air. Free to use and transfer. Owned and issued by the people and NOT the State! (Corcoran, 2013)

As the slogan of the Bitcoin Foundation, 'Freeing People to Transact on Their Own Terms', clearly states, the anonymity of transactions and the decentralized organization aim, in particular, at forbidding public powers from interfering in private transactions. The system is meant to eliminate all intermediaries that may potentially intervene in the creation and the circulation of money. Yet despite these discourses intermediaries still proliferate and forms of regulation, more or less irregularly distributed, develop as Bitcoin's intervention and influence in the global monetary system unfolds.

Bitcoin as a currency comes out of its sphere of exclusivity when some of the actors in its ecosystem make Bitcoins convertible: its value becomes the subject of speculation, and becomes volatile. These two features, volatility and convertibility, have jointly facilitated misappropriations, hijacks and détournements. Wannabe Bitcoin thieves target primarily those venues that are known to host a big quantity of Bitcoins: exchange platforms, which have become not only very powerful operators in the Bitcoin market, but also its points of weakness(xi). This phenomenon has led to a number of questions related to regulation, and to the exploration of solutions for the organization of Bitcoin exchanges, both from public authorities and civil society actors.

The price (and risk) of connection

At the moment when Bitcoin is convertible, it becomes de facto inter-connected with the external monetary system, and becomes comparable with other monetary devices. A system of money calibration takes shape; exchange rates are published; variation curves are made public; and, within a general trend of growth, dramatic increases and crashes appear(xii). From the time we begun to write this paper in January 2013 to its last revisions a year later, the rate has soared from $20 to $930. This variability of the course is immediately read as related to the trust that users place in the currency, while it feeds both mistrust and trust itself at the same time.

The first crash in 2011 can be explained in several ways, but in particular it is linked to a speculative bubble, grounded in very human dynamics of enthusiasm, involvement, and fear – the confrontation of a technical system designed to function without intermediaries with the universe of speculation and its hazards. As Wallace concisely puts it:

> Even the purest technology has to live in an impure world. (Wallace, 2011)

> As the currency made more headlines around the globe (including in The Economist), less techie types wanted in on the action. Then […] they decided to cash in, and the bubble burst. (The Economist, 2011)

The intervention of other intermediaries further amplifies the magnitude of the variations and the volatility. The media, for example, both relays and magnifies these effects. Thus, the most rapidly increasing peak of interest in Bitcoin, the June 2011 shift from 9 to 30 USD, seems closely correlated (if not caused) by Gawker's article on Bitcoins' acceptance by illegal online marketplace, Silk Road (Wallace, 2011).

Bitcoin has recovered from those two major crises. Yet legal scholar Reuben Grinberg warns that loss of confidence as both cause and consequence of Bitcoin's volatility is perhaps one of the structural weaknesses of the system, and one that it will have to reckon with as long as it exists:

> Bitcoin is probably susceptible to irrational bubbles and also irrational or rational loss of confidence, which would collapse demand relative to supply […] confidence might collapse in Bitcoin because of unexpected changes in the inflation rate imposed by the software developers or others, a government crackdown, the creation of superior competing alternative currencies, or a deflationary spiral. (Grinberg, 2011)

For other analysts, though, cracks happen for causes that are internal to the system, such as when the system has been faced with too heavy a volume of transactions. On the occasion of the second big crack in Bitcoin's history (early April 2013), founder of Bitpay Tony Gallippi remarked to the Financial Times that that the problem may reside in people's attempts to conduct bigger transactions than Bitcoin can handle (Foley, 2013). The Economist directly relates the strong decline in Bitcoin's course to primarily technical problems of data handling and updating:

> As more users join the network, the amount of data that has to circulate among them (to verify ownership of each Bitcoin) gets bigger, which slows the system down. Technical fixes could help but they are hard to deploy: All users must upgrade their Bitcoin wallet and mining software (…) the currency could grow too fast for its own good. (The Economist, 2013)

This unregulated fluctuation also draws the attention of public authorities to Bitcoin. Some of them try to intervene, with limited success:

> A Bitcoin exchange operating in France has been adjudged to be the subject of European Banking rules. Practically, this has had little impact on the average European's ability to exchange Euros for Bitcoins in Europe. (Elias, 2011)

The connection to the 'real world' of financial speculation is also the cause of hijacks. Convertibility is the cause of the majority of incidents concerning Bitcoin. One of the most serious episodes concerned, in September 2012, the theft of 24,000 Bitcoins (roughly $250,000) from Bitfloor, which is an exchange platform of a smaller size than the major actors such as MtGox(xiii). The firm's CEO recounts:

> Last night, a few of our servers were compromised. As a result, the attacker gained accesses to an unencrypted backup of the wallet keys (the actual keys live in an encrypted area). Using these keys they were able to transfer the coins. This attack took the vast majority of the coins BitFloor was holding on hand. As a result, I have paused all exchange operations. Even tho only a small majority of the coins are ever in use at any time, I felt it inappropriate to continue operating not having the capability to cover all account balances for BTC at the time. (Bitcointalk, September 4, 2012)

Taking advantage of an unencrypted backup, thieves had 'transferred' Bitcoins on accounts that the anonymity of the system prevents from retracing. There was nothing the intermediary, Bitfloor, could do faced with the disintermediation of transactions, and it found itself in the situation of having to cover the whole set of misdirected transactions and compensating all its Bitcoin-holder clients. Other hijacks or attempted thefts are mentioned in literature: MtGox, for example, was forced to temporarily suspend its exchange operations after a massive distributed denial of service (DDoS) attack in June 2011.

In the distributed definition of responsibility taking shape in Bitcoin, unfair behaviours only have repercussions on their victims, be they direct or indirect. To avoid damaging the trust of users, intermediaries are forced to cover their losses and mark a discontinuity between the encryption, whose integrity must not be doubted, and the transactions of which they assume responsibility.

A weak regulation?

Faced with cracks, steep variation curves, and misappropriations, voices have called for a regulation of exchanges. Important actors complain about the juridical void in which Bitcoin is located. MtGox takes "a step towards complying with US money-laundering regulations by registering as a money services business with the US Treasury Department" (Bonney, 2013), while the Treasury's Financial Crimes Enforcement Network, known as FinCen, has established a code of good conduct for exchange agents (Sidel, 2013).

Indeed, in addition to the major conceptual shift it requires Bitcoin is a system very difficult to grasp legislatively for national and international institutions – and it is so by design. The insertion of Bitcoin in current

legal frameworks is an open and important issue for it to operate as a legitimate and trustworthy service. All the more so as some of Bitcoin's features lend themselves to attracting unethical or fraudulent behavior by some companies:

> There are several important legal aspects, such as data protection and privacy, consumer protection, contractual and private international law issues, e-commerce legislation including liability issues in virtual worlds, and the financial regulatory aspects, know your customer etc. Neither the Bitcoin website nor the text of its software license shed any light on this. Well, not much anyway. (Jacobs, 2011)

> [There are] problems associated to tax evasion and fraud because of the impossibility of calculating the official value of the transaction in what can be considered, technically, a barter economy. (Brezo & Bringas, 2012)

A history of public authorities' (failed or unsuccessful) attempts to regulate P2P and decentralized exchanges in the past through traditional enforcement means speaks to the detriment of a hypothetical application to Bitcoin of such or similar means:

> Bearing in mind past efforts to crack down on P2Pnetworks such as BitTorrent, Pirate Bay, etc it is obvious that the regulatory authorities may face a challenge enforcing anything on Bitcoin. (Jacobs, 2011)

Alongside these unfinished attempts at regulation by public authorities, users of the Bitcoin network (in particular, businesses; Mendoza, 2012) get organized in order to allow practices that more accurately mirror the system's initial 'calling'. A number of arrangements and devices begin to act as intermediaries, and contribute to the performance of the money's creation and circulation: statistics on exchange volumes, bug maintenance features, the recognition of specific discussion forums as 'official'. And the Bitcoin Foundation, a non-profit registered in Washington, DC, is born with the objective of "help(ing) people exchange resources and ideas more freely", and three practical missions: the standardization of Bitcoin (particularly its code), the protection of its encryption protocol, and the promotion of the Bitcoin currency in the public space. As we see, two out of three among the Foundation's intermediation functions are focused on code: its resilience, its standardization, its harmonization.

The complexity of the Bitcoin system is such that not only the technology itself but also the people behind the technology need to be entrusted with the users' confidence. Indeed, there is an important amount of technical and political control which software developers may exert upon the decentralized system, by shaping transaction anonymity, the uniqueness of Bitcoin addresses, and the privacy-by-design embedded in the network.

It appears that the forms of intermediation and regulation that are currently developing will not only address the currency's broader system of inscription (its circulation, its exchange rules…), but, as they have started to do, they will also act upon the heart of the system: the code. The intermediaries of the Bitcoin system help bring to light the ways in which the code, as the technical heart of the system, and its modalities of application, daily practices, and incarnations in political and social actors are intertwined, and not easily separable. Modifications in the algorithm, so that an increased number of transactions can be managed, affects the very core of the system. Thus, it becomes impossible to separate – in the analysis, and in practice – the trust that users bestow upon the monetary system as a whole (of which Bitcoin becomes an element among the others) from the trust in the code.

Conclusions

During its brief, lively, and volatile history so far, one of the most interesting ways that Bitcoin has questioned the status quo of the monetary system has been to challenge the need of institutional guarantors in the building of monetary trust. Yet, contrary to the alleged original intentions of Bitcoin's developers, monetary trust is not (and perhaps cannot be?) disposed of. Rather, a 'distributed trust' is performed via a number of socio-technical devices, embedded in the underlying P2P architecture of the system. In this article, we have followed how experts in different disciplines account for a number of devices and dynamics by means of which distributed trust is built in Bitcoin. This sheds light on the plurality of ways in which currency can be understood. Currency can indeed be understood via the link it builds between the devices involved in its use, and the conceptions of the value it embodies. Expert knowledge contributes to the very definition and shaping of trust within the Bitcoin system, ultimately contributing to perform the shared definition of its value.

Because of the innovations it proposes to bring to the daily practice and very concept of currency, the Bitcoin system provides an especially interesting laboratory of analysis for these issues. Indeed, not only do the four sets of dimensions we have analysed in this article shed light on how distributed trust is built, preserved, and tested; they also shape different definitions of what actually constitutes trust. And they ultimately suggest, somewhat paradoxically, that Bitcoin's gradual insertion into the 'real world' – the monetary and economic systems it was born against – actually contributes to the emergence of the forms of trust that permit its stabilisation.

The analysis of the different dimensions of distributed trust we have proposed here is based on a survey of expert discourse. An extension of our work will be to continue this type of investigation on other types of discourse. Our hypothesis, to be further put to the test, is that the issues we have highlighted associated with the development of a decentralized trust at least partially overlap with those that analyses of other corpuses would make visible. In particular, we are thinking of Bitcoin's technical support forums, which constitute the privileged entrance door into the very particular world of Bitcoin and will provide further elements of analysis on trust-building processes vis-à-vis this currency.

Footnotes

(i) This work is part of ADAM (http://adam.hypotheses.org/), a multidisciplinary research programme on distributed network architectures and its applications to different organizational and communication systems, funded by the French National Agency for Research (ANR, CONTINT programme ANR-10-CORD-000).

(ii) According to https://blockchain.info/fr/.

(iii) Economists classically understand money by means of three functions: it is a reference point, allowing to measure and compare the value of goods; an intermediary in commercial exchanges; and a reserve of value. Blanc (2009) underlines a fourth function indicated by Karl Polanyi, the ability to conduct payments that are not, stricto sensu, a counterpart of commercial exchanges: taxes, fines, tributes. This fourth function is relevant as it helps accounting for the strong role of money and currency in redistribution processes, that represent, in Polanyi's work, a crucial aspect of the link between economy and society (Polanyi, 1957).

(iv) http://bitcoinmagazine.com/

(v) To give but a few examples in these different categories:

https://www.weusecoins.com/, https://bitcoinfoundation.org/?, https://github.com/bitcoin/bitcoin?, bitcoin.stackexchange.com/?, bitcoin.org/? and the national declinations of the Bitcoin forums such as http://www.bitcoin-italia.net/ and www.bitcoin.fr/?.

(vi) 53 results in Web of Knowledge (http://wokinfo.com/) in January 2013.

(vii) http://www.scirus.com/

(viii) As a simplification, we consider here the case of a user who wants to exchange directly within the network. Today, there are intermediary service providers who provide Internet users with "Bitcoin electronic wallets" that they manage on users' behalf. In this case, the user does not need to connect the machine directly to the P2P network, and merely transmits transaction orders to the service provider – and the latter does, indeed, need to be connected to the network.

(ix) Maurer et al. (2013) give PayPal, a company that secures its own revenue by 'ensuring' transactions, as an example.

(x) Interestingly, this notion is borrowed from the civil code to better assess responsibilities, and locate the debate in a legal perspective.

(xi) According to the press, the most important of these platforms, MtGox, has conducted up to 80% of Bitcoin transactions – and still conducts half of them today.

(xii) E.g. an increase of 500% in two months in the summer of 2011, and the course halved in the following weeks.

(xiii) Just before the release of this issue, in February 2014, MtGox has suspended trading, closed its website and exchange service, and filed for "civil rehabilitation", a form of bankruptcy protection from creditors.

Bibliography

Aigrain, P. 2010. Declouding Freedom: Reclaiming Servers, Services and Data. In 2020 FLOSS Roadmap (2010 Version/3rd Edition), https://flossroadmap.co-ment.com/text/NUFVxf6wwK2/view/

Akrich, M., M. Callon and B. Latour. 2006. Sociologie de la traduction. Textes fondateurs. Paris: Presses des Mines.

Androulaki, E., G. Karame, M. Roeschlin, T. Sherer, S. Capkun. 2012. Evaluating User Privacy in Bitcoin. IACR Cryptology ePrint Archive 2012: 596.

Bauwens, M. 2005. The Political Economy of Peer Production. CTheory.net. Available at http://www.ctheory.net/articles.aspx?id=499

Blanc, J. 2009. Usages de l'argent et pratiques monétaires. In Traité de sociologie économique, ed. Steiner, P. and F. Vatin, Paris: PUF.

Bonney, J. 2013. MtGox registers with FinCEN as a money services business. CoinDesk, June 29, 2013. Available at http://www.coindesk.com /mt-gox-registers-with-fincen-as-a-money-services-business/

Brezo, F. and P. G. Bringas. 2012. Issues and Risks Associated with Cryptocurrencies such as Bitcoin. SOTICS 2012: The Second International Conference on Social Eco-Informatics.

Callon, M. 2007. What does it mean to say that economics is performative? In Do economists make markets? On the performativity of economics, ed. MacKenzie, D., F. Muniesa and L. Siu, 311-358. Princeton, NJ: Princeton University Press.

Callon, M. 1986. Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay In Power, Action and Belief: A New Sociology of Knowledge, ed. Law, J., 196–233. London: Routledge.

Callon, M. et al. 2013. Sociologie des agencements marchands. Paris: Presses des Mines.

Callon, M., C. Méadel and V. Rabeharisoa. 2002. The economy of qualities. Economy and Society 31, 2: 194-217.

Corcoran, T. 2013. Gold vs. Bitcoin : Which one is a true safe haven ? Financial Post, April 13, 2013. Available at http://opinion.financialpost.com/2013/04/16/terence-corcoran-gold-versus-bitcoin/

The Economist. 2013. Virtual currencies : Mining digital gold. Print edition, April 13, 2013. Available at http://www.economist.com/news/finance-and-economics/21576149-even-if-it-crashes-bitcoin-may-make-dent-financial-world-mining-digital

The Economist. 2011. Virtual currencies : The bursting of the Bitcoin bubble. October 21, 2011. Available at http://www.economist.com/blogs/babbage/2011/10/virtual-currencies

Elias, M. 2011. Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy. Working Paper. Available at SSRN: http://ssrn.com/abstract=1937769 or http://dx.doi.org/10.2139/ssrn.1937769

Foley, S. 2013. Bitcoin fans put brave face on price fall. Financial Times, April 12, 2013. Available at http://www.ft.com/cms/s/0/4118322c-a389-11e2-ac00-00144feabdc0.html#axzz2av45roeY

Graeber, D. 2011. Debt: The First 5000 Years. New York, NY: Melville House.

Graeber, D. 2001. Towards an Anthropological Theory of Value: The False Coin of Our Own Dreams. New York, NY: Palgrave.

Grinberg, R. 2011. Bitcoin: An Innovative Alternative Digital Currency. Hastings Science & Technology Law Journal, 4(1): 159-207.

Ingham, G. 2004. The Emergence of Capitalist Credit Money. In Credit and State Theory of Money, ed. Wray, R., Cheltenham: Edward Elgar.

Ingham, G. 1996. Money Is a Social Relation. Review of Social Economy, 54, 4: 507-529.

Jacobs, E. 2011. Bitcoin: A Bit Too Far? Journal of Internet Banking and Commerce, 16, 2.

Jansen, M. A. 2012. The political 'virtual' of an intangible material currency. MA thesis, Utrecht University.

Kaplanov, N. M. 2012. Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation. Temple University Legal Studies Research Paper. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203

Latour, B. 1988. The Pasteurization of France. Cambridge, MA: Harvard University Press.

Maurer, B. 2006. The Anthropology of Money. Annual Review of Anthropology, 35: 15-36.

Maurer, B., T. C. Nelms and L. Swartz. 2013. "When perhaps the real problem is money itself": the practical materiality of Bitcoin. Social Semiotics 23, 2: 261-277.

Mendoza, N. 2012. Bitcoin Business and Trust. Bitcoin Magazine, October 2012.

Mendoza, N. 2013. The Other Side of a Bitcoin: P2P Welfare in Bitcoin Country. Bitcoin Magazine, January 2013.

Moglen, E. 2010. Freedom In The Cloud: Software Freedom, Privacy and Security for Web 2.0 and Cloud Computing. ISOC Meeting, New York Branch, 5 February 2010.

Musiani, F. 2013. Nains sans géants. Architecture décentralisée et services Internet. Paris: Presses des Mines.

Nakamoto, S. 2009. Bitcoin : A Peer-to-Peer Electronic Cash System. Working Paper. Available at http://bitcoin.org/bitcoin.pdf

Noizat, P. 2012. Bitcoin, une devise complémentaire universelle. ParisTech Review, January 2012.

Orléan, A. 2009. La sociologie économique de la monnaie. In Traité de sociologie économique, ed. Steiner, P. and F. Vatin, 210-246. Paris: PUF.

Orléan, A. 2007. Croyance monétaire et pouvoir des banques centrales. Working Paper, Paris School of Economics. Available at http://www.parisschoolofeconomics.com/orlean-andre/depot/publi/banques0701.pdf

Polanyi, K. C. M. Arensberg and Harry W. Pearson. 1957. The place of economics in societies. In Polanyi, K. 1957. Trade and market in the early empires; economies in history and theory, Glencoe IL: The Free Press.

Salyer, K. 2013. Bitcoin's a Revolution, Not a Convenience. Bloomberg Opinion, June 4, 2013. Available at http://www.bloomberg.com/news/2013-06-04/bitcoin-s-a-revolution-not-a-convenience.html

Sidel, R. 2013. Bitcoin Investors Hang On for the Ride. The Wall Street Journal, April 16, 2013. Available at http://online.wsj.com/article/SB10001424127887324345804578426692340390104.html

Simiand, F. 1934 (2006). La monnaie, réalité sociale. Annales Sociologiques, Série D. Paris, Alcan. (New edition : Critique sociologique de l'économie, Marcel J.-C. and P. Steiner, Paris : PUF).

Wallace, B. 2011. The Rise and Fall of Bitcoin. Wired, December 2011. Available at http://archive.is/oODpb

Zelizer, V. 1997. The Social Meaning of Money: Pin Money, Paychecks, Poor Relief, and Other Currencies. Princeton, NJ: Princeton University Press.