10/2016

Moving mountains with the digital wind

Eric Arrivé

Abstract

As digital technologies become ever more reticulate, it has become conceivable to implement communication protocols that express certain ideals of justice. These protocols would be designed and used to redistribute to users power that had become concentrated in the hands of certain players such as governments or big companies. Cryptocurrencies are an example of this kind of protocol, Bitcoin being the one most used today. However, a detailed analysis of this protocol, and in particular the principle of "proof of work" that lies at its heart, shows that it falls a long way short of putting users back in control of their interactions. This analysis can be extended to digital technologies in general, the spread of which can be interpreted as the effect of a blind dynamic generated by their bifid character. Just as with the kind of commodity production criticised by Marx, the effects produced by this type of dynamic are real, but its fetishistic nature effects a reversal in which the abstract – in the form of indifference to content – overrides the practical uses claimed by their promoters. Within this irrational and unconscious framework, the quest for any form of justice by means of digital protocols becomes illusory.

Introduction

Whether with promises of new democratic forms or, conversely, warnings about the potential for antidemocratic control, digital networks have prompted extensive discussion on the impact and role they might have in the emergence of new modes of governance and power distribution (Loveluck, 2015a). The reticulation of digital technologies has, however, come to be taken so much for granted that questions about them have been confined to this particular realm. While the increasingly networked nature of these technologies has unquestionably introduced a new object

of examination, their unprecedentedly rapid spread nevertheless began well before, arousing debate on the future they might presage.

For example, the possibility of digital tools becoming a source of justice was challenged on the grounds of the asymmetry between actors, at a time when a distinction was being drawn between the "large cauldron" and the "small cauldron" (Lussato, 1982), a reference to the then emerging alternative between centralised computing and personal computing. This technical choice was seen as having the potential to steer events towards a greater or lesser degree of justice and liberty, because behind this alternative lay the difference between reinforcing the role of the dominant players (states and big companies like IBM at the time), or letting individuals and small structures develop in complete autonomy.

Today it is the architecture of digital networks (De Filippi and Bourcier, 2014) that is the battleground between the abuse of a dominant position by the powerful and those who see distributed digital architectures as the way to their dissolution. Amongst the applications that depend on this kind of architecture, cryptocurrencies – at least in the eyes of their promoters – constitute the ideal framework for establishing fair interactions between their users. Without prejudging whether the technical proposals advanced and implemented truly back up this claim for justice, the question of whether the form of justice thus promoted is really neutral remains open. Much more fundamentally, however, with respect to the claimed objectives, is this not an illusory question in the absence of a critical analysis of the techniques employed? It is a question that arises in particular with regard to the territorial disruptions wrought by the required infrastructures.

I will begin by presenting the promoters of cryptocurrencies, identified with the "Californian ideology" critically analysed by Barbrook and Cameron (1996). But beyond the mobilisation of an ideology to promote a more or less explicit agenda of social transformation, I will situate these arguments as one expression amongst others of a wider though unspoken belief about the specificities of the form of capitalist social synthesis, notably in relation to money. I will then move on to the principles whereby cryptocurrencies operate, with a focus on the case of Bitcoin, a

virtual currency system that employs a peer-to-peer network and cryptographic functions as the basis of a competition to produce "proofs of work". I will then show that the dynamic generated by this system produces effects that are not confined to a virtual world. I then proceed to an analysis of the formal framework of this dynamic, an analysis that can be applied to all digital techniques and compared with the dynamic generated by commodity production. Finally, through a commentary on Karl Marx's *Fragment on Machines*, I will explain this comparison and demonstrate the irrational character of that dynamic.

The promoters of cryptocurrencies

Cryptocurrencies have been in existence for less than a decade, but their current development is continuous with the upheavals brought about by the spread of digital technologies in the field of information and communications since the 1980s. This spread has been driven by a community of engineers, entrepreneurs and artists, but also theoreticians in the human and social sciences, who see the computer as the ideal tool to optimise interactions within society, on the basis of a very particular vision of those interactions.

A nonarbitrary currency?

Cryptocurrencies are an attempt to produce – by exploiting the possibilities afforded by digital technologies – currencies devoid of all the imperfections that are the legacy of historical currencies, and – according to their promoters – to retain only the properties appropriate to the optimum (and fair) operation of a currency. This is accomplished, again according to these promoters, by cutting out the operators who ultimately acquire controlling power over the users of the currency, whether they are the states that issue that currency – and are therefore guarantors of its survival – or banking and financial intermediaries.

Cryptocurrencies clearly fall into the "private currency" category since, in their very conception, they are neither issued (directly or indirectly), nor guaranteed, by a state. In this respect, they are actively promoted and developed by those who, in line with

the views promulgated by Friedrich Hayek (1976), seek the means to diminish the capacity of states to manipulate the economy to their advantage. The fundamental form through which the notion of private currency is understood is the contract, but an *anonymous* contract that enables it to be used as a method of payment founded and circulated solely on the basis of supply and demand. This "contractualism" echoes the theory of justice developed by John Rawls (1987), but is also opposed to it in its rejection of any redistributive role assigned to the state (Nozick, 1988).

The ideal of justice claimed by the promoters of private currencies is thus founded on transparency, the only guarantee of an undistorted application of the principles of supply and demand. Behind this claim there is a vision of the user of the currency as a rational economic agent relying on open information to reach decisions that maximise his interests. The irrationality and manipulations introduced by the state (and by the institutions to which the state delegates management of the currency) as a privileged agent that abuses a power perceived as illegitimate and opaque, is contrasted by the adherents of private currencies with the rational and self-interested action of individual agents who openly and public produce an equilibrium of optimum benefit to all.

The Californian ideology

In the case of cryptocurrencies, these positions held by the promoters of private currencies are reinforced by the fact that the latter form part of a population heavily involved in the implementation of information and communication technologies (ICT). The development of ICT is advanced as the general framework within which innovations can ultimately lead to the large-scale adoption of private currencies.

It was studies dating from the late 1990s, such as those of Barbrook and Cameron (1996), Winner (1997) and Borsook (2000), which revealed what came to be called the "Californian ideology". The more recent work by Turner (2006) added unexpected historical depth to this phenomenon, notably by showing how 1960s counterculture ideas contributed to the development of digital technologies, despite their origin at the time in laboratories contracted to the U.S. Army.

"The Californian ideology" is the belief that ICT will dissolve existing power structures and replace them with direct interactions between autonomous individuals by means of software alone. Any interference with these elementary interactions is even proclaimed as inviting the kind of pushback that those who defy the laws of nature must expect. In a sense, this ideology can be summed up by the idea that *computerisation is liberation.*

Throughout history, people…

If the promoters of cryptocurrencies claim to be deploying a new currency – and even a new generation of money – it is therefore a claim based on a particular understanding of what a currency is (or should be). Other opposing conceptions of currency could be advanced (Aglietta & Orléan, 2002, Testart, 2001), notably characterised by the stipulation that a currency is necessarily attached to an institution that establishes its validity. Despite mutual rejection of their respective premises, these contradictory positions nevertheless share a common principle with the adherents of cryptocurrencies: that there exists a general and trans-historical concept of currency on the basis of which a generic and standard role can be assigned to it, whether in ancient Greek (or even older) societies or in modern industrial era societies. Although possible discontinuities may be identified and emphasised, they are nevertheless situated in historical contexts and social forms where the categories used to characterise them remain problematic. The emergent phenomenon is thus applied beyond the historical and social conditions of its emergence. While it may take a succession of forms, it nevertheless follows an evolving pattern that is claimed to demonstrate the permanence of a common principle (Herrenschmidt, 2007).

Currency is therefore understood as a given, quasi-anthropological and recurrent, stable in its foundations, perhaps varying in its forms, but whose underlying meaning is established from its first emergence and which varies only in its superficial manifestations, whether contingently or evolutively. This means that the most recent developments differ only in their derived and purely technical functions, notably in

the expansion of the financial sphere or the virtualisation of monetary exchanges. In this view, historical variations merely correspond to the emergence of increasingly sophisticated – but also purer – methodological forms employed to achieve quasi-natural ends, such as the circulation of goods or information. The objection that can be made to these diverse and irreconcilable positions is that they share a reductive bias: the retro-projection onto precapitalist societies of categories that are specific to that particular form of social synthesis.[1] The specificities in question are both absent and omnipresent in the currency theories corresponding to these antagonistic positions: absent because not challenged, omnipresent because they constitute the framework into which phenomena that relate to other explanations are compressed.[2]
It is not the purpose of this article to establish what theory of money would be most appropriate to analyse the emergence of cryptocurrencies. The aim is more to establish how this phenomenon stands in a very particular form of social synthesis. So while it is important to remember that a trans-historical concept of money primarily expresses a socially and historically situated form of consciousness, this claim for a new currency embedded in new media can be interpreted from two complementary perspectives. First, as the mark of "the illusion of the moment" regarding a phenomenon wrongly considered to be a reality that is transposable from one form of social synthesis to another, and secondly as the sign of a new phase in the form of social synthesis in which this claim is expressed.

The principles of cryptocurrencies

Contrary to what the term might suggest, cryptocurrencies do not refer to currencies that are hidden in shadow or exchanged in secret. Quite the contrary, they are

1"It went without saying for the modernity established in the West that the forms of socialization specific to it, and their categories, are systematically dehistoricized and ontologized" (Kurz, 2015, 95).

2 Jacques Le Goff (2010) notably shows that money in the Middle Ages was the development of a social nucleus (*caritas*) that is irreducible to the economic categories in which we place it today. The mediaeval form of social synthesis expresses drivers and meanings through currency that make it a phenomenon that cannot be attached to the category "money", which proves to be specific to the societies of modernity.

founded on the public exposure of shared information and messages disseminated openly via digital networks. Later on, we will look at the nature, the mode of production and the use of this information in these messages. The term "crypto" instead refers to the fact that their implementation depends on cryptographic algorithms, though their purpose is not secrecy.

Indeed, while cryptography is a discipline dedicated to the security of information, confidentiality (and therefore secrecy) is only one aspect of it. The cryptographic functions that underpin the operation of cryptocurrencies fall into two other categories: authenticity and integrity. The purpose of the first is to ensure that the message actually comes from the associated source. That of the second, to ensure that the message has not been modified since it was sent.

Innovations that have reached maturity

The last 10 years have seen the maturing of different IT protocols through which cryptocurrencies are implemented. Together, these protocols form a class of applications founded on common principles: the use of digital cryptography, as cited above, peer-to-peer networks and the notion of "proof of work"[3] (Jakobsson and Juels, 1999, Back, 2002). Bitcoin is one of these protocols (Nakamoto, 2009),[4] so far the most highly developed in terms of the size of its network (number of participants) or monetary valuation, and in fact the one most cited in the media.

3 Some cryptocurrencies replace the "proof of work" mechanism by other forms also founded on digital calculation, such as "proof of stake". I will not cover these variants in this article, since they represent a minority of cryptocurrencies and their relevance is largely contested by the promoters of Bitcoin.

4 Bitcoin simultaneously refers to a unit of account employed in monetary transactions and the IT protocol that defines the way in which monetary fractions are produced and exchanged via digital networks. By tacit agreement in the community of users and developers, "Bitcoin" with a capital is used for the protocol, while lowercase "bitcoin" is used for the unit of account. In order to avoid ambiguity in the rest of this article, I will employ the terms "Bitcoin protocol" for the first and "bitcoin currency" for the second, when necessary.

The money supply represented around 14.7 million bitcoins when this article was written (October 2015). The exchange rate is around US$245 for one bitcoin, which means that the total is valued at more than US$3.6 billion. The daily trading volume is around 300,000 bitcoins, i.e. approximately US$74 million.[5]

In this article, I will give a succinct description of the protocol in a way that will bring out properties that are not claimed by its promoters, but nevertheless explain the dynamics of its spread more accurately than the self-proclaimed perfection of the monetary exchanges that rely on it.

A peer-to-peer network

The Bitcoin protocol can first of all be seen as a protocol that defines the messages to be exchanged and the tasks to be accomplished by different digital algorithms – programs executed by computers – communicating over a peer-to-peer network (Musiani, 2015). By definition, the topology of this kind of network allows each participating algorithm (also called a "node") to potentially enter into communication with any other.

Moreover, in the case of Bitcoin, the network is decentralised, which means that this communication is established without first passing through a particular node that holds the information concerning the network map. In reality, a message sent by one node will first be distributed to a few nearby nodes, known to the sender. The messages received by a node can in turn be resent from these first recipients to nodes other than the initial sender.

By this mechanism, it is enough that a few nodes be directly accessible, for any node to be able to send a message, from one node to the next, which will reach all the nodes in the network. This can be accomplished without the network topography being known to any node, and even functions when – unknown to the nodes – that

5 Data accessible at https://blockchain.info/fr/charts. The website *blockchain.info*, amongst others of the same kind, e.g.(http://btc.blockr.io), trawls the information contained in the register of Bitcoin transactions, and provides access to certain statistics built around this information. It is an illustration of the fact that the data relating to transactions are indeed open and public.

topography is shifting. The sender is content to launch the message nearby and leaves the responsibility for propagating it to the network itself.

At present, the implementation of the Bitcoin network relies on Internet infrastructures. Wherever the Internet is accessible, the Bitcoin network is as well. There are currently more than 5000 nodes spread around the world, though mainly located in the USA (around 35%), in Germany (around 11%) and in France (around 7%) (source: https://bitnodes.21.co).[6]

A non-localised resource

The role assigned to the network is to keep an up-to-date ledger of the transactions carried out since its launch at the beginning of 2009. To do this, each node holds a copy of the ledger and communicates to the others, through the exchange of peer-to-peer messages, all additions – and only additions, because modification and deletion are impossible – of which it is notified. The role of the nodes is also to verify the validity of these additions before disseminating them to their peers. The operations to be carried out for this validation are defined in the Bitcoin protocol that each node implements, so that the propagation of these additions from one node to the next builds a consensus regarding that validity, and therefore regarding the content of the ledger at any time.

Here, therefore, we find a mechanism to establish a database that is non-localised but nevertheless consistent – in the sense of robust, coherent, non-contradictory – regardless of the access point, allowing for a reasonable time lapse. In fact, the average propagation time for a message about an addition to the ledger was estimated in 2013 to be a dozen seconds, and 95% of the nodes were reached in less than 40 seconds (Decker and Wattenhoffer, 2013). More recent data indicate that these propagation rates have since remained within the same order of magnitude,

6 This website provides information on the Bitcoin network by collecting public data supplied by the nodes. It is a creation of the firm 21 Inc., a start-up that designs and sells machines dedicated to the "production" of bitcoins. These machines contribute to the Bitcoin network by performing a task called "mining", which is described later on in this article.

from a few seconds to a few dozen seconds (source: http://bitcoinstats.com/network/propagation). Moreover, plans for "clouds" of dedicated low-orbit microsatellites are also under consideration, in order to reinforce the resilience and robustness of the network (source: http://www.dunveganspace.com/bitsat.html)

Authentication and integrity

A second aspect of the Bitcoin protocol consists in the use of cryptographic functions to construct the information contained in the ledger. As previously indicated, the functions are not intended to mask this content but to fulfil two services essential to the functioning of an account ledger.

First of all, the function is to authenticate the stakeholders in each transaction. In the case of the Bitcoin protocol, this authentication entails an identifier rather than a name. Indeed, the identifier does not refer to a particular person but to previous transactions of which the person may be the anonymous beneficiary. This identifier is thus used to check the validity of the transfers – the balance corresponding to the identifier is reconstructed by running through the history of the transactions involving that identifier – and to restrict access to the bitcoins to their legitimate holders: it is enough to hold a key that is associated with the identifier and employed to release the funds for use in subsequent transactions. It may be noted that "ownership" of the bitcoins depends solely on the possibility of providing this key when one wishes to transfer them. If the key is lost, the bitcoins become inaccessible. If another person acquires the key, they can use the bitcoins. No appeal is possible under any circumstances.

The second role fulfilled by the cryptographic functions is data integrity. The aim is to guarantee that these data have not been altered between the time they were produced and the time they are accessed. In technical terms, authentication and integrity are maintained in the Bitcoin protocol by digital signature mechanisms that are a mix of asymmetric encryption and a hash function (Antonopoulos, 2014). I will

return in greater detail to the hash function, which is also used in the third aspect of the Bitcoin protocol, i.e. calculating a proof of work.

Proofs of work

The last aspect of the Bitcoin protocol concerns the way in which the entire network agrees on the data to be added to the transaction ledger. While we have already seen, first, how the data are constructed on the basis of cryptographic functions, and secondly how the network disseminates these data to all the nodes by peer-to-peer notifications, we have yet to describe how the consensus is established on the data that will constitute a new addition to the account ledger. The problem to be solved in order to establish a certain level of trust in these data is how to prevent a malicious user successfully adding fraudulent transactions. To do this, all the actors must be able to cooperate, despite the fact that there is no central authority to organise that cooperation. So a mechanism is needed that allows each of them to act separately and also encourages them to do so "honestly". The crucial innovation introduced by the Bitcoin protocol lies in the use of "proofs of work" within a peer-to-peer network.

One way to describe the mechanism is as a lottery in which a draw is made on average every 10 minutes. The participants in this lottery are once again digital algorithms. They carry out an aspect of the Bitcoin protocol called "mining" and the operators they control are called "miners". These incongruous terms – for an apparently virtual task – are used to refer to the activity of those who take part in the lottery by "extracting" *proofs of work*: essentially, this means unearthing a nugget by trawling through large quantities of uninteresting "virtual material". Let us look in more detail at the sequence performed by a "mining" algorithm and what underpins the notion of proof of work as material for extraction.

Initially, the "mining" algorithm receives, via the peer-to-peer network, the transactions sent by Bitcoin currency users. Each "miner" collects these transactions and assembles them into a "to-be-processed" list. When a "mining" operation begins, the "miner" takes a number of these transactions for processing and assembles them into a new "processing list". Then it calculates a value from the elements in this list

and a randomly generated number, which together constitute what is called a block. The calculation in question is based on a so-called "hashing" function defined by the protocol and the resulting value is a fingerprint of the assembled data.

A hash is a cryptographic function with the following properties: on the one hand, it provides a numerical value contained within a preset interval regardless of the size of the input data, and on the other hand, small variations in input data produce large differences between the corresponding values calculated. These properties, combined with the fact that the interval between the calculated values is quite large, mean that each value calculated can be defined as a unique fingerprint that can only have been produced by a specific set of data. Another property of the hashing function is its practical irreversibility: calculating a hash is a relatively simple and cheap operation; however, determining what data will produce one hash or another is a practically impossible task.

The task of the "miner" is to vary the random sequence included in the block, until it finds a hash code that represents a value below a limit set by the Bitcoin protocol, called a "target" value. This limit is set in such a way that the calculation only rarely arrives at an appropriate value. Given the properties of the hashing functions, the "miner" has no other practical solution than to produce an astronomical quantity of variations in the random sequence, repeating the calculation each time. While each calculation is fast and inexpensive, the repetition needed to arrive at the right hash value eventually takes up significant time and computing capacity. It is therefore assumed that by finding an acceptable value, the "miner" has demonstrated that significant effort has been expended[7]: this is what is called proof of work.

When a miner finds an appropriate value, it broadcasts the result of the calculation on the Bitcoin network. By the mechanism of peer-to-peer transmission, all the other

7 In fact, the notion of proof of work was initially developed with the aim of preventing "denial of service" type attacks against online services, by making their cost prohibitive (Back, 2002). In these attacks, the service provider is "inundated" with an avalanche of requests that monopolise its resources. The counter is then to require a proof of work before responding to each of the requests. For a genuine user, this proof of work will remain painless, but it would oblige an attacker to commit resources that would exceed the expected reward.

"miners" are quickly informed that a winner has, so to speak, been drawn out of the hat. Each of them checks the validity of the data in the winner's block, adds it to the copy of the transaction ledger they hold and withdraws the transactions featuring in the winning block from their "to-be-processed" list. This sets off another race to "mine" the next block.[8]

While checking the proof of work simply consists in (re)calculating the hash of the winning block and therefore requires few resources, it is clear that this is not the case for the winner who finds that block. How then can "miners" be encouraged to participate in the gradual and shared construction of the transaction ledger, if it costs them? The answer is once again in the Bitcoin protocol, which provides two mechanisms. First, "miners" have the right to include, in the blocks they produce, a transaction that credits them with a certain amount of bitcoin currency defined in the Bitcoin protocol. This itself provides an ongoing source of newly created currency.[9] And second, when the input amounts of a transaction are greater than its output

8 Another piece of data that has so far not been mentioned appears in the winning block and is also one of the elements used in calculating the hash. This is the hash of the previous block. This series of blocks can therefore be seen as a chain – called the *blockchain* – in which each element reinforces the proofs of work of the people who use it. This cumulative effect multiplies the irreversible character of the proof of work mechanism, since this not only relies on the total computing power available at a given moment to build a block, but also progressively entails all the computing power implemented for the blocks that follow it.

9 It should be noted that the bitcoin currency supply is limited by the protocol to 21 million bitcoins. The issue of bitcoins is itself programmed over time according to an asymptotic function, by the fact that the number of bitcoins a miner can credit to themselves is halved approximately every four years. For Bitcoin's promoters, this limit is offset by the fact that its value in fiat currency will increase to reflect the computing power mobilised on the network, and thereby the robustness of the information contained in the blockchain. This idea that the intrinsic value of the bitcoin (and of any currency) is connected, directly or indirectly, to a standard that corresponds to a physical magnitude, is open to criticism. Marx (2015) had already shown that money was not based on an underlying standard, but emerged as a universal merchandise on the basis of the generalised practice of commodity exchanges, hence only in a very particular type of society. As commdity, bitcoin can in fact be classified in the "type 2 commodity" category (Lohoff and Trenkle, 2014). This is undoubtedly a more relevant starting point for explaining the trend in the bitcoin rate since its creation.

amounts, miners have the right to collect the difference as optional fees for their contribution to the operation of the network. Transaction originators have an incentive to leave this "tip" because miners will prioritise the processing of transactions that contain it.

Finally, the last point regarding proofs of work, the "target value" that a block's hash must reach is a floating parameter, constantly adjusting to the total computing power available on the network as a whole. This target varies in inverse proportion to that of computing power, and is adjusted in such a way that the average time between the discovery of two winning blocks remains 10 minutes. This 10 minutes interval is a fixed parameter in the Bitcoin protocol. The floating parameter that varies with total computing power (therefore inversely with the target) is called "difficulty".

An emergent dynamic

On the basis of the description of the Bitcoin protocol provided in the section above, I will demonstrate that the protocol contains a dynamic that is an emergent property of the combination of its different parameters, and more specifically the parameters that set the framework for the production of proofs of work.

Competition as a driver

The production of proofs of work takes place within a competitive framework. The minimum computing power that a "miner" has to employ for mining to be a profitable activity is correlated with the total power available on the network by means of the floating parameter of "difficulty". Every new mining entrant therefore has to align themselves with this minimum level in order to succeed. Nonetheless, the more computing power a miner has, the better their chances of winning. Indeed, reward is allocated with a level of chance proportional to the ratio between the miner's individual computing power and the total power in the network. This incites the competitors to add power individually, which in turn simultaneously adds to the total computing power, and therefore helps to raise the "difficulty" and therefore to

reduce the chances of winning for all the competitors. In order to align themselves again with this new level of "difficulty", while continuing to be profitable, all the miners will look for new technical solutions that will make mining more productive. These solutions will ultimately spread to all the mining operators, and those who are unable to implement them will be automatically excluded from the game and eventually disappear.

A blind and impersonal dynamic

The Bitcoin protocol therefore intrinsically generates a dynamic that drives an indefinite increase in the total computing power employed on the network and constant and ever faster upgrades to the underlying technologies. This dynamic is not driven by any specific operator but by the interplay of competition between them all. In the absence of any external limiting factor, the result is exponential increase. This is what occurred, for example, between October 2013 and October 2014, when the "difficulty" multiplied by a factor of more than 180, whereas total computing power rose from two trillion hashes per second to more than 300 trillion (source: https://blockchain.info/fr/charts/difficulty et https://blockchain.info/fr/charts/hash-rate). Since then, the rate has slowed as a result of constraints that were not the outcome of a decision to regulate the phenomenon, but of physical limits that (temporarily?) imposed a more linear rate of increase between October 2014 and October 2015. These limits mainly arise from the fact that the equipment currently used for mining has incorporated all the possible short-term innovations to improve productivity,[10] and that medium-term innovations require a higher level of investment than the market actors are currently able to take on. However, whatever the rate, it is clear that no deliberative rationality is applied to defining the process of increase, let alone to managing it.

10 I describe these innovations and their sequences later in the article. They are essentially developing in two directions: first with microelectronic engineering, which is developing specialised processors with the aim of improving calculation speed (generally expressed in billions of hashes per second) relative to power consumption; and second with the industrial concentration of computing capacity in dedicated "factories", subject to location constraints specific to digital technologies.

Real material effects

Although the Bitcoin protocol, like every formal protocol, seems to belong exclusively to the virtual realm, its implementation via digital techniques also anchors it in material phenomena from which it cannot be detached without in fact preventing its implementation and thereby consigning it permanently to the realm of blue sky ideas. This materiality is made up of the millions of computers engaged in running "mining" algorithms.

Environmental impact

The computer is a machine driven by an engine and designed to cause rearrangements of matter. It consumes electrical energy to produce digital calculation in the sense ascribed to it by Turing (Girard, 1995), i.e. the step-by-step execution of transitions between the machine's different internal states. Although miniaturisation makes these transitions imperceptible to human senses, they are nevertheless material phenomena and computation would be impossible without this physical medium.

The numerous environmental impacts of the development of digital technologies are now well-known (Dobré, Flipo, Michot, 2013), whether in terms of electricity consumption, extraction of the required materials or waste accumulation. The consequences for human societies are also well documented, notably armed conflicts for the control of coveted resources.

Technical obsolescence

In the space of scarcely seven years, the "mining" infrastructures employed on the Bitcoin network have already undergone three big transitions, each associated with a change in the type of processors employed by "miners" for calculating hashes. The processor is the computer's core component, the central processing unit. This component's internal architecture can be designed with varying degrees of "rigidity", in order to optimise its performance with regard to a given class of algorithm.

During the initial phase, computing power was provided by individuals using computers built around "conventional" mass-produced processors (CPU). Then, more specialised machines were introduced, using processors dedicated to graphics operations (GPU). The tasks for which these processors are designed and optimised require an internal architecture which is more effective for the hash computation employed in mining bitcoins. The next step was the use of a new category of so-called "programmable" processors (FPGA). These processors are in a sense devoid of any internal architecture, which is only defined subsequently by a designer after manufacturing. This technique produces processors with a generic physical substrate that can be optimised for a particular type of algorithm. Finally, the last stage is to incorporate into the initial design of the processors itself the capacity to run specific algorithms with maximum possible efficiency. This entails the development of specific integrated circuits (ASIC) dedicated to hash computation.

Each transition provided an opportunity to enhance computing power per processor, while reducing per-unit electricity consumption. With the most recent generation, however, a limit to the possibilities of processor architecture has been reached. Improvements are possible, but they will remain within the same technical lineage and will focus only on marginal reductions in per-unit consumption. While the smallest material gain offers a competitive advantage that can continue to drive obsolescence, the priority for competitors today is nevertheless to reduce operating costs. To achieve this, they look to concentrate their infrastructures as close as possible to the cheapest energy sources.

New industrial locations

The geographical distribution of the Bitcoin network's nodes – those simply responsible for keeping a copy of the transaction ledger – is concentrated (source: https://bitnodes.21.co) in the countries historically associated with the emergence of digital technologies (both as designers and producers of hardware and software and as markets for the consumer goods produced). By contrast, the distribution of

"mining" power shows that two thirds of it is now concentrated with four operators[11] (*F2Pool, AntPool, BTCChina Pool and BitFury*, source: https://blockchain.info/pools), the first three of which are Chinese and operate *datacenter* type infrastructures spread all over the world.[12] In an infrastructure of this type, a large number of computers (to the order of several tens of thousands of units, sometimes more) are concentrated in a single location, with the aim of standardising and optimising their operation. Obviously, for reasons of profitability, the criteria for deciding the location of these infrastructures are primarily access to a low-cost source of electricity and the possibility of dissipating the heat produced efficiently. These criteria sometimes lead to choices that are, at first sight, surprising, but unanswerably logical from the perspective of the development of digital technologies. So for example, the Chinese company HaoBTC which, having built facilities in Inner Mongolia because of its cheap and plentiful coal, is now setting up in Tibet in order to exploit that country's even more competitive hydroelectric resources, at the price of a geographical isolation that is comparable in industrial history only with nuclear plants, but for clearly quite different reasons (source: http://www.coindesk.com/my-life-inside-a-remote-chinese-bitcoin-mine).

A concrete/abstract dialectic

A calculation without specific content

For bitcoin miners, hash computation – a mass process that lies at the core of the Bitcoin protocol – is a function with no specific content. Indeed, it delivers no particular result but contributes to the purely formal production of an abstract entity,

11 These operators are "pools", i.e. aggregators of computing power: they bring together several thousands of "miners" in order to combine their computing power and redistribute the rewards in proportion to each miner's contribution. Each "miner" receives a higher return on the power they supply, but has to renounce the possibility of choosing the blocks they mine.

12 BitFury, for example, has announced that it plans to invest $100 million in the construction of a datacenter in Tbilissi, capital of Georgia (source: http://bitcoin.fr/bitfury-investit-100-millions-de-dans-un-nouveau-data-center).

proofs of work. Independently of the real transactions carried out by Bitcoin users, for these "miners" the hashing function becomes an end in itself (at an ever higher level of efficiency) and produces effects on and by the resources employed, which are unquestionably real.[13]

There are therefore two sides to the Bitcoin protocol, whose interaction is the very essence of its logic. On the one hand, there is a tangible side, in the sense that it addresses a particular need, which is represented by transactions carried out by users of the bitcoin currency. The real-world scope of this aspect begins and ends with the use made of the Bitcoin protocol by the "contracting parties". On the other hand, there is an abstract side, in the sense that it is empty of specific content, which is represented by the "qualityless" computing power deployed by the "miners" in order to produce proofs of work indefinitely, regardless of the content of the transactions processed. This side, which shows an *indifference to* (and not *detachment from*) any specific content, generates a dynamic and proves crucial in ultimately explaining the observed real-world effects, above and beyond those pursued by the protocol's promoters.

Mirror of the computer itself…

Indifference to content is not, however, specific to the Bitcoin protocol, which may be seen as an avatar of computational reason (Bachimont, 2006), a reason itself reliant on formalisms alone.

The formula is a process that is used to reason on the basis of form alone, without the need to pay attention to meaning. Since the form embodies in its structure what is needed from the meanings considered, it is enough to manipulate the form in order to conduct reasoning about content or meaning. […] Relying on form is the

13 The total power dedicated to bitcoin mining as of 26 October 2013 was 36,080 petaflops (see http://bitcoinwatch.com/) (1 petaflop = 10^{15} floating point operations per second). This is more than 1000 times the power of the world's most powerful computer (China's Tianhe-2), which only manages 33 petaflops, and it is significantly more than the combined power of the 500 most powerful computers. That's a lot! What may be seen as an enormous waste of computing power will get worse if bitcoin wins […] (Delahaye, 2013, 80)

attitude at the basis of all formalisms, in particular those that underpin the computer sciences […] (Bachimont, 2006, p.9)

However, Bachimont says nothing about the necessity of having to rely on a concrete application in implementing computing technology. It is not simply about manipulating form in the blue sky of ideas, but manipulating it in relation to a use, even if the latter is ultimately restricted solely to its formal aspects during the manipulation. There is therefore a genuine dialectic between the concrete and the abstract which drives the real-world development of digital techniques (Arrivé, 2015).[14]

… And of commodity production

This type of dialectic was extensively explored by Karl Marx (2015) in his analysis of commodity production, and in particular his – fundamental – analysis of the labour that produces commodities. New readings of these analyses, positing the commodity-form as the foundation of the modern form of social synthesis, have been advanced by Moishe Postone (2009), who notably shows the non-contingent nature of the industrial techniques determined by capital. Further light can however be cast on the case of digital technologies through a commentary on a passage in the famous "Fragment on Machines", one of the preparatory works (Marx, 2011) for the writing of *Das Kapital*.

In it, Marx refers to the future of the means of labour as capital,[15] i.e. the fact that the totality of the means mobilised in capitalist production are determined by this mode

14 The reader is referred to this article for a more detailed analysis of the bifid aspect of digital technologies, which simultaneously show two sides, which can neither be separated nor reversed: "The genericity of the computer therefore reflects two aspects, two facets, like the two sides of a single coin, which mark the specificity of the computer: on the one hand, a general character arising from the ability to run any formal procedure, and on the other hand a generative character through the fact of realising this potential by running a particular procedure with universal scope, which can itself produce any one of the totality of conceivable particular cases."

15 The means of labour represents all the technologies implemented in the production of goods, whether these technologies are material or immaterial, individual equipment or continental-scale

of production. On the one hand, in its material existence, this totality follows a necessary trajectory which is that of industrial technologies. On the other hand, in its formal existence, this cumulative and constantly renewed totality itself becomes fixed capital, and is therefore indissolubly connected with the movement of capital in general.

In the machine, and even more in machinery as an automatic system, the use value, i.e. the material quality of the means of labour, is transformed into an existence adequate to fixed capital and to capital as such; and the form in which it was adopted into the production process of capital, the direct means of labour, is superseded by a form posited by capital itself and corresponding to it. (Marx, 1973, p.692)

It may already be noted that the industrial mechanism represented by the totality of digital means of production follows this same process. As a means of automating production,[16] it is a part – at a higher level of integration – of the machinery that constitutes the necessary – and itself necessarily in movement – body of capitalist production. This totality also exists formally as fixed capital, which may take multiple forms, be it *datacenters*, patents or databases. Likewise, computing technology produces – at new scales in both extension and depth – an encapsulation effect, i.e. the disappearance within black boxes of the physical and formal principles that govern the machinery and in turn influence users who are quite incapable of understanding its operation, and therefore the origin of the effects of which they can be no more than observers.

The science which compels the inanimate limbs of the machinery, by their construction, to act purposefully, as an automaton, does not exist in the worker's consciousness, but rather acts upon him through the machine as an alien power, as the power of the machine itself. (Marx, 1973, p.693)

infrastructure, such as power or information networks. It may, for example, consist of a chemical conversion process, a power transmission device, or indeed the rationalised organisation of an assembly line.

16 Indeed, digital technologies have introduced new consumer objects that have become a ubiquitous presence in our everyday lives, but less spectacularly, these technologies have above all been used for the rationalisation of production processes.

"What acts" in the case of computing technology is all the more difficult to grasp in that there are multiple levels of encapsulation. First because its materiality is embodied in the infinitely small, at imperceptible scales. Then because of action at a distance, i.e. the possibility that the machine that acts and its effects are not "in presence". And finally, because the effects are increasingly perceived as modifications to the environment rather than as chains of cause and effect, even at the level of speculation (Rouvroy and Berns, 2013).

So while computing technology may be a new phase in the machinery of production (and while moreover its equipment is not strictly situated in units of production), this machinery should nevertheless first be understood as a stage in a historical process driven by the dynamics of capital.

The development of the means of labour into machinery is not an accidental moment of capital, but is rather the historical reshaping of the traditional, inherited means of labour into a form adequate to capital (Marx, 1973, p.694).

As Marx indicates in the remark above, it must nevertheless be recognised that this process is not just a material accumulation, but also the process whereby capital is brought into formal correspondence with itself. The most adequate form that fixed capital could take at the time when Marx was writing the *Grundrisse*, which would continue until the end of Fordism, was that of industrial machinery as a use value employed in the production of commodities. While it might have seemed the most adequate form in the initial phase, it does not exhaust the possibilities of a more advanced correspondence.

Machinery appears, then, as the most adequate form of fixed capital, and fixed capital, in so far as capital's relations with itself are concerned, appears as the most adequate form of capital as such.[17] In another respect, however, in so far as fixed capital is condemned to an existence within the confines of a specific use value, it

17 In the composition of capital, Marx distinguishes two interacting parts: constant capital representing the assets designed for use in production processes (machines, patents, raw materials…) and variable capital representing the force of living labour employed in that same process. In addition, he makes another distinction between fixed capital (in the form of lasting goods) and circulating capital (in the form of raw materials and wages).

does not correspond to the concept of capital, which, as value, is indifferent to every specific form of use value, and can adopt or shed any of them as equivalent incarnations (Marx, 1973, p.694).

In the case of digital technologies, this machinery is no longer captive in its own existence as use value, since materially it possesses a side that is indifferent to any set form of use value. At every moment of the machinery, its entire universal potential can be expressed through a particular use that actualises it. Likewise, each of these moments is employed both for the use value that it provides but also, simultaneously, for the abstract totality that it helps to cover.

A fetishistic form?

Just as Marx exposes the fetishism that results from the commodity-form, i.e. the real inversion between concrete and abstract, in which the concrete becomes simply an indifferent medium for the tautological and irrational deployment of the abstract (Postone, 2013), a similar conclusion can be drawn from digital technologies, the case of Bitcoin being one illustration. The notion of "proof of work" in the latter case is an (ironic) reminder of the role that labour for the production of commodities plays in the modern social synthesis, which makes any rational "management" – whether by machines or by a political process – totally illusory, since this synthesis happens "behind the backs" of the participants (Jappe, 2012).

Conclusion

In his book *Réseaux, libertés et contrôle. Une généalogie politique d'internet*, Loveluck (2015b) shows the connection between liberal political economy and approaches that attempt to take account of informational factors in the age of digital networks. It was notably with the work of Benkler (2009) that this connection was demonstrated, the title of his book *The Wealth of Networks* echoing Adam Smith's *Wealth of Nations.* In this liberal tradition, the goal of the analysis of political economy is to determine the fairest conditions for the distribution of the fruits of social activity. By contrast, the Marxist critique, set out in the first chapters of *Das*

Kapital, consisted in analysing the basic categories of political economy (labour, money, commodity…) – and not in providing the elements of a fairer alternative political economy – in particular by showing their fetishistic character as the unconscious and irrational product of a generalised activity (commodity production) grasped solely in its phenomenal dimensions (the circulation of commodities).

From the moment it becomes possible to identify a similar fetishistic character in the emergence of digital technologies, the liberal vision of the political economy of digital networks demands the formulation of a critique capable of linking the phenomena observed to the profound driving forces that underpin the development of these particular techniques. It is perhaps time – i.e. both possible and necessary – for the emergence of a critical volume that could bear the title "*Das Komputal*". This would provide a framework for the explanation of how digital technologies are now capable of generating effects as powerful as "moving mountains" – in a non-metaphorical sense – in a continuing attempt to annihilate space (Laumonier, 2013). It would also be an opportunity to explore whether any justice is truly conceivable through a tool which, in its deployment, constitutes a mere indifferent medium that nevertheless consumes every kind of physical, psychic and symbolic resource.

About the author: Eric Arrivé, PhD candidate - ELICO - Lyon 2 University

To quote this article: "Moving mountains with the digital wind", *justice spatiale* | *spatial justice*, n°10, June 2016, http://www.jssj.org

Bibliography

Aglietta Michel & Orléan André, *La Monnaie entre violence et confiance,* Odile Jacob, 2002

Antonopoulos Andreas, *Mastering Bitcoin,* O'Reilly Media, 2014

Arrivé Eric, « Du caractère fétiche des techniques numériques », dans *Interfaces Numériques Vol 4/3*, 2015

Bachimont Bruno, « Signes formels et computation numérique : entre intuition et formalisme », en ligne http://www.utc.fr/~bachimon/Publications_attachments/Bachimont.pdf, 2006

Back Adam, « Hashcash – a denial of service counter-measure », en ligne http://hashcash.org/papers/hashcash.pdf, 2002

Barbrook Richard, Cameron Andy, « The Californian Ideology », dans *Science as Culture 6:1 (janvier)*, p. 44-72, 1996

Benkler Yochai, *La richesse des réseaux*, PUF, 2009

Borsook Paulina, *Cyberselfish. a critical romp through the terribly libertarian culture of high tech*, PublicAffairs, 2000

Decker Christian, Wattenhoffer Roger, « Information Propagation in the Bitcoin Network », *13th IEEE International Conference on Peer-to-Peer Computing*, 2013

De Filippi Primavera, Bourcier Danièle, « Réseaux et gouvernance. Le cas des architectures distribuées sur internet », *Pensée plurielle 2014/2 (n° 36), p. 37-53*, 2014

Delahaye Jean-Paul, « *Bitcoin*, la cryptomonnaie », dans *Pour la Science n°234*, 2013

Dobré Michelle, Flipo Fabrice, Michot Marion, *La face caché du numérique*, L'Echappée, 2013

Girard Jean-Yves, *La machine de Turing*, Éditions du Seuil, 1995

Hayek Friedrich, *The Denationalization of Money*, Institute of Economic Affairs, 1976

Herrenschmidt Clarisse, *Les trois écritures, langue, nombre et code*, Gallimard, 2007

Jakobsson Markus, Juels Ari, « Proofs of Work and Bread Pudding Protocols », dans *Comms and Multimedia Security 99*, Chapman & Hall, 1999

Jappe Anselm, « Peut-on s'émanciper du fétichisme ? », conférence du 26 octobre 2012 à l'université de Lausanne dans le cadre du colloque Penser l'émancipation. Théories, pratiques et conflits autour de l'émancipation humaine, 2012

Kurz Robert, « La fin du politique », dans *Cités* 2015/4 (N° 64), p. 93-110.

Laumonier Alexandre, *6*, Zones sensibles, 2013

Le Goff Jacques, *Le Moyen-Âge et l'argent*, Perrin, 2010

Lohoff Ernst et Trenkle Norbert, *La grande dévalorisation*, Post-éditions, 2014

Loveluck Benjamin, « Internet, une société contre l'État ? Libéralisme informationnel et économies politiques de l'auto-organisation en régime numérique », *Réseaux 2015/4 (n° 192), p. 235-270*, 2015a

Loveluck Benjamin, *Réseaux, libertés et contrôle. Une généalogie politique d'internet*, Armand Colin, 2015b

Lussato Bruno, *Le défi informatique,* Sélect, 1982

Marx Karl, *Grundrisse, Foundations of the Critique of Political Economy*, Penguin, 1973

Marx Karl. *Le Capital livre I, Le développement de la production capitaliste*, Éditions sociales, 2015.

Musiani Francesca, *Nains sans géants - Architecture décentralisée et services Internet*, Presses des Mines, 2015

Nakamoto Satochi, « Bitcoin: A Peer-to-Peer Electronic Cash System », en ligne http://www.bitcoin.org/bitcoin.pdf, 2009

Nozick Robert, *Anarchie, État et utopie*, PUF, 1988

Postone Moishe, *Temps, travail et domination sociale,* Mille et une Nuits, 2009.

Postone Moishe, *Critique du fétiche capital, PUF*, 2013.

Rawls John, *Théorie de la justice*, Éditions du Seuil, 1987

Rouvroy Antoinette et Berns Thomas, « Gouvernementalité algorithmique et perspectives d'émancipation », dans Réseaux 2013/1 (n°177), 2013

Testart Alain (dir.), *Aux Origines de la Monnaie*, Errance, 2001

Winner Langdon, « Cyberlibertarian Myths and the Prospects for Community », en ligne http://homepages.rpi.edu/~winner/cyberlib2.html, 1997