books & ideas.net

The Bitcoin El Dorado

By Ludovic Desmedt & Odile Lakomski-Laguerre

Conceived by its inventors as the basis of a new monetary order, Bitcoin seems to have been overtaken by finance and become the object of lucrative speculation.

Almost ten years after Bitcoin was launched, the French Finance Ministry would like, with the help of France's Financial Markets Authority and flexible and incentivizing regulation, to make Paris the most attractive financial center for ICOs (Initial Coin Offerings), those cryptocurrency fundraisers that experienced record growth in the first trimester of 2018. In early January, other countries, including China and South Korea, hardened their position towards this new ecosystem, while digital currency projects have been either already launched at the level of individual states (such as the Petro in Venezuela) or announced as under development by major central banks (notably the Bank of England). Is the cryptographic currencies revolution a threat1 or a genuine innovation that could lead to new opportunities for growth? Can Bitcoin still be considered as a monetary alternative or has it become, despite erratic price fluctuations, the financial world's new El Dorado?

Bitcoin, a monetary techno-utopia?

Following the economic troubles provoked by the 2008 crisis, the image of financial institutions was tarnished, and criticism and complaints about bank-created money grew: it led

[1] The Bank for International Settlements (which is, in a sense, the central banks' bank) has just published a 24-page report ("Cryptocurrencies: Looking Beyond the Hype") that lambasts cryptocurrency as a product prone to "risk," "instability," and which involves "vast energy use"!

to excess debt, took financialization too far, and brought speculation and instability. At the practical level, numerous initiatives were launched along the margins of the official system, giving birth to alternative forms of exchange. The latter brought to light the fact that currency is in fact heterogeneous and pluralistic, thus undermining dominant representations and traditional conceptualizations of currency as centralized, homogeneous, and sovereign. In 2009, in a document delineating the operating principles of a new digital currency, Satoshi Nakamoto (2009) asserted:

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.

According to "him" (Nakamoto is in reality a pseudonym, behind which hide one or several conceptualizers), the automatization of the issuing of means of payment within a voluntary community of users makes it possible to avoid "conventional" currency's shortcomings. The coding ("crypto") protocols introduce a new logic of inter-agent transfers: a simple peer-to-peer agreement suffices to make payments, with cryptography ensuring optimal security.

Thus Bitcoin has nothing to do with other monetary alternatives, such as local and complementary currencies, which were also developed in the crisis' wake. It is a payment instrument that seeks to be international, supported by disruptive technology and organized as a network. It thus constitutes a paradigm reversal vis-à-vis bank-created money and the way it is regulated, which makes it possible to imagine a new monetary order in the history of payments. Since the protocol conceived by Nakamoto was open access, it gave considerable scope to the emergence of a universe of competitive and unregulated private currencies. Today, there exist more than 1,500 cryptocurrencies (such as Litecoins, Ripple, Ether, Dogecoin, etc.), and the total value of these instruments is estimated at more than 300 billion dollars.2 The project closely resembles what the liberal Austrian economist Friedrich Hayek imagined in his 1976 book The Denationalization of Money, in which he envisioned the possibility of a founding a solid monetary order on the virtues of competition and the free market, with the (major) difference that, in Hayek's scenario, banks would remain the issuers. In May 2018, a "Declaration of Monetary Independence" began to circulate on the internet, challenging the monopoly of the "old system" (i.e., states and banks) in this domain.3

Nearly ten years after its creation, Nakamoto's project, which Nigel Todd describes as a "techno-utopia," betrays a fundamental ambivalence: monetary alternatives and contestation are now in retreat, in favor of an increasingly financial logic. This financialization of the cryptocurrency world undoubtedly represents a major trend in contemporary capitalism, from

[2] "The amount to crypto-assets in circulation reached around €330 billion in late January 2018, consisting primarily of Bitcoin (35%), Ether (20%) and Ripple (10%)," Banque de France, 2018, p. 3. Since March 2018, the Banque de France recommends the use of the term *crypto-actifs* ("crypto-assets") for the English term "cryptocurrencies."
[3] See http://currencyindependence.com/index.html.

which no realm of activity seems able to escape. But it is also the result, in our view, of a conjunction between problems of conception, a new technology that is the object of considerable (speculative) envy, and a discourse about cryptocurrency put forth by a group of actors with an interest in ensuring that it loses its initial monetary purpose.

This elimination of the monetary dimension of Nakamoto's project occurred in two ways. First, Bitcoin quickly became dissociated from its technology, blockchain, which was increasingly emphasized. This technology, which has been described as genuinely revolutionary (almost as revolutionary as the internet), enjoyed extraordinary publicity even as Bitcoin's image remained scandal-ridden due to its use on the darknet. Companies and investors saw blockchain as harboring possibilities that go beyond monetary transactions—indeed, the properties of the distributed register that is blockchain make it possible for any document, asset, or digital signature to be authenticated, stored, and transferred—and the general enthusiasm for this technology overtook some of the original ideas in Nakamoto's paper, which was devoted to the creation of an alternative payment system. Recently, after the speculative bubble of late 2017 and at a time when the purely financial activities tied to the advent of these new technologies have grown, the term "crypto-asset" has emerged, replacing that of "cryptocurrency" and marking a significant semantic shift, notably in the discourse of official monetary authorities.

Yet Bitcoin was conceived as a payment system: the protocol defined a unit of account, as well as a set of rules and procedures governing the issuing and transfer of monetary units and the security of transactions. The original texts and most of the websites devoted to it refer primarily to Bitcoin's role as "means of payment": its goal is to define a new monetary space, thanks to computer networks that have been liberated from banking, regulatory, and fiscal burdens, among others. The original project was in fact a monetary protest, the roots of which lie in the world of anarchist cryptographers, who wanted to preserve individual freedom and protect private data through a currency that cannot be easily traced (see Desmedt, Lakomski-Laguerre, 2015).

The financialization of Bitcoin and money's ambivalence

The fact remains that access to Bitcoin occurs primarily through the sale of official currencies on specialized trading platforms at a market price that fluctuates with supply and demand. In this way, digital money becomes one currency among others and its value can be determined by its exchange rate, rather than by some inherent value (since the end of the dollar's gold convertibility in 1971, no currency can be expressed in terms of a base good). Whereas in 2011 Bitcoin's price peaked at $0.10, since 2011 its rise has been extraordinary, attaining a few symbolic peaks, the most recent of which occurred in the summer of 2017, when it hit nearly

$20,000. The expectation of controlled supply (the protocol ensures that Bitcoins will be issued on an automated basis, with the total capped at 21 million, a figure that will be reached in 2040), which is able to meet a potentially growing demand, should inevitably result in the digital currency's appreciation and constitute, in this way, a great incentive to hoard it and use it for speculative investments.

If the interest of new users has a major influence on the volume of Bitcoins sold on trading platforms, the impact is, however, weak and even non-existent on the volume of exchanges in the system. Put differently, those who buy Bitcoins for the first time have no intention of using them as an alternative currency for spending. This phenomenon was also encouraged by cryptocurrency's connection to—one might even say absorption by—the financial world. Thus when in late 2017 the Chicago Stock Exchange launched a derivative product making it possible for investors to protect themselves from Bitcoins' price fluctuations, this sent a positive signal to the financial community from a publicity standpoint, but also contributed to characterizing cryptocurrency as an asset. More recently, the significant growth in start-up financing techniques through "initial coin offerings" has further anchored cryptocurrency in the logic of finance.

This speculative dimension, which has been widely promoted by the media, thus massively attracted actors who saw Bitcoin, Ripple, Ether, and others as nothing more than opportunities for quick and easy monetary gains.

As for the monetary dimension, the network still has some technical difficulties to overcome relating to congestion, which considerably slows down the speed at which transactions can be finalized (sometimes taking up to a week) and significantly increases transaction costs (thus vitiating one of the primary commercial arguments for using digital currency). For cryptocurrencies to become commonly used, they must be able to process a load of several thousand transactions per second. Yet it is possible to imagine ingenious methods for mitigating these difficulties, as well as technical innovations, such as those being developed by Lightning Network. It is also possible to assume that the currency will evolve toward a very different use, with a portfolio consisting of a range of cryptocurrencies devoted to specific uses. Yet in this type of competitive environment, one must also assume that users would have at their disposal all information relating to currency-issuers, so as to optimize their portfolios on the basis of these various currencies' values. Is this possible? Is plurality not naturally inclined to introduce further complexity?

For now, the relationship between these two dimensions, payment and investment, is problematic and relates to what Michel Aglietta calls "the ambivalence of money": a currency is a public good that ensures the proper functioning of payment systems, whereas finance relates to the valorization and private appropriation of wealth. Within a particular monetary domain, the relationship between means of exchange and store of value is normally harmonious, but pathologies can emerge: the store-of-value dimension can subside (as with inflation), or it can dominate and "block" exchange (as with hoarding). If hoarding prevails, the financial dimension

can threaten payments. In such cases, according to the German philosopher Georg Simmel, money is rendered "immobile."

Some have described Bitcoin as "digital gold," but the Midas myth reminds us that a dangerous fascination with metals can paralyze exchange: for the past several months, the number of transactions in cryptocurrencies has been in steep decline. Consequently, some have announced Bitcoin's imminent demise, while others already consider it obsolete, compared to the many innovations in this domain that are occurring at an impressive pace. Others see Bitcoin as nothing more than a speculative bubble that will burst sooner or later (its price has experienced a serious correction between late December and the present), a big scam, or just a flash in the pan. Perhaps. Yet it is worth remembering, for all who are interested in history's lessons, that bank-created currency, at its beginnings, also underwent considerable turmoil, as evidenced by (to cite two traumatic French experiences) the assignats debacle during the French Revolution and the collapse of John Law's bank (which was tied to speculative euphoria). Some time was subsequently required before the public's trust in bank currency was firmly secured.4 But beyond the debate between zealots and detractors, those who are interested in monetary questions see the emergence of cryptocurrencies as a fascinating subject, one that requires us to re-examine our vision of the economy and society. What is money? What is its essential role in the economy? Is monetary competition sustainable over the long term? Can one imagine a lasting currency without a state or any form of centralization?

Is trusting the code enough?

If one admits that some cryptocurrencies could become future modes of payment, what conditions would have to be in place for a monetary order to arise? French institutionalist approaches to currency (see Aglietta, Orléan, 1998; Alary, Blanc, Desmedt, Théret, 2016) have identified a few clues and brought attention to forms of trust, which guarantee that a particular monetary instrument is anchored in the collectivity. We will confine ourselves here to addressing two of them: hierarchical trust and ethical trust.

Hierarchical trust refers to an acknowledged relationship of subordination to a superior authority, which defines the rules according to which this currency will be used (and has the power to change them) and guarantees the means of payment and value of monetary signs,

[4] 210 years prior to Nakamoto's project, in 1798, *Le Journal des Débats* informed its readers that they could see, displayed on Rue de l'Université in Paris, "ingenious machines that served to make paper money, among which one may admire Richer's mechanical numbering machine, which, solely through the movement of a printing press line, can change every number, according to their natural order, from 1 to 9999" (Bourgueil, 1798, p. 394). Beginning at this time, automatization and coding shaped currency emission protocols. Automatization did not, however, prevent the *assignat* disaster.

while also protecting users against possible failure. Robust technical procedures and blockchain's non-falsifiability (in principle, at least) supposedly guarantees the quality of payments. In this model, the idea is to do away with any form of hierarchical authority (banks, central banks, and the state). But the protocol upon which Bitcoin is founded, after Nakamoto disappeared, was confined to a community charged with ensuring the digital currency's development and the promotion. Consequently, the trust being considered here relates both to the code and to the coordination and governing of the community, which, aside from users, consists of three types of key actors: miners, developers, and exchange platforms. Other systems, such as Ripple, are managed by private companies. How are these actors coordinated? Who decides? How are rules modified? How are crises managed? Who really holds power? No serious thinking about Bitcoin can avoid these questions. The Bitcoin community recently grappled with a conflict relating to a modification of the protocol to increase block sizes due to network overload. In March 2017, Morgan Phuc of BitConseil concluded:

> The Bitcoin community must find a consensus between its economic axis (the incentive model and the transaction fee market), its security axis (the protection of the integrity of actions), and its ideological-political axis (the governance of the ecosystem) … The question of how the various actors (developers, miners, exchange platforms, and users) will govern the system persists, and, as it faces important decisions, the community must act in a coordinated and decentralized way to honor Satoshi Nakamoto's legacy.5

Ethical trust, for its part, refers to the values that monetary relations promote. As has been seen, the network is based on libertarian values and seeks to emancipate itself from arbitrary political decisions by avoiding manipulative abuses on the part of the state: anonymity, transparency, and decentralization lie at the heart of the ethical and commercial model of cryptographic currencies.

The first two principles have an ambivalent relationship to one another and may conflict with the public's conception of a legitimate currency. First, while the system touts its anonymity and the protection of private data, and while some users do join for the right reasons (to fight the censorship of dissident positions, to seek protection from abuses of power and control, and so on), it must be admitted that this kind of instrument attracts a parallel (i.e., fraudulent, illicit, and criminal) economy that can have a lasting impact on potential users' trust. Bitcoin still has the reputation of a scandal-ridden currency, as evidenced by its association with Silk Road (a website that is particularly associated with online drug sales). More recently, Bitcoin has become the "official currency" in which digital pirates demand their ransoms, as occurred during the vast cyber-attacks of May 2017.

While it is easy to argue for Bitcoin's criminal potential, this reasoning is not especially cogent: there already exists a significant underground and criminal economy financed by cash, not to mention the banking system's involvement in tax havens. Bitcoin does not,

[5] http://bitconseil.fr/Bitcoin-guerre-blocs/.

moreover, guarantee total anonymity. For while the use of pseudonyms for payments masks one's identity, blockchain's public character makes it possible, however, to display the history of each Bitcoin and of portfolio-related activities. Furthermore, in February 2016, the European Commission decided, among other measures, to include virtual currency exchange platforms in its anti-money laundering directive and to subject them to the requirements relating to identification and identity verification provided for by European regulation. Bitcoin is thus becoming less and less of an anonymous currency. Consequently, to satisfy a public that is very concerned with preserving confidentiality, other solutions have been proposed: two new, concurrent cryptocurrencies that guarantee anonymity, Zcash and Monero, are growing increasingly popular.

Decentralization, for its part, seems to be the Bitcoin system's key innovation, in addition to being one of the main reasons its first users chose this kind of instrument. Decentralization avoids power concentrations that would allow a single individual or organization to take control. It also tends to make a computer system available and resilient, by ensuring there is not a single point of failure. Yet this decentralization seems more theoretical than actual. Major economic forces have in fact pushed for the centralization and concentration of a small number of intermediaries at different levels of the ecosystem. At least three important categories of intermediaries, who have shaped digital currency's evolution, are affected by this centrifugal force: miners, exchange platforms, and digital portfolio services companies. Concentration is also the result of capital amassed in Bitcoins benefiting minorities. In absolute terms, this tends to distort the original ethical model, which was unique to peer-to-peer groups and favored a cooperative approach. But such concentration also proves problematic for price evolution mechanisms, since the market is not atomistic, but strongly reactive to the operations of a small handful of actors with enough capital to have a significant impact on prices.

For now, it is difficult for to say what will become of the world of cryptocurrencies: over the past two years, the strategies of regulators, commercial and central banks, and states have evolved considerably. Consider two examples: Ripple, launched in 2012 by Ripple Labs, experienced the largest price increase of 2017 (+36,000%). Founded on the blockchain protocol, this cryptocurrency has become an instrument for interbank payments that facilitates international transfers between commercial institutions. Over time, Ripple could replace the SWIFT system established in 1973.6 It is also known that the world's primary central banks are now experimenting with procedures for settling balances through blockchain, and several scenarios for rethinking payment systems in their totality are being studied (see Pfister, 2017). Finally, several (more or less serious) projects for cryptocurrencies at the state level are under development: the Petro, launched in Venezuela amidst debilitating inflation, is not likely to have staying power, but could give the country access to foreign financing. Estonia and other countries are, it seems, working on more viable protocols, but these projects for

[6] The Society for Worldwide Interbank Financial Telecommunication seeks to ensure standardized formats for transfers between institutions and allows central banks, commercial banks, and financial institutions to exchange information and make transfers electronically.

developing "sovereign" cryptocurrencies are contrary to the original philosophy of alternative networks. In these ways, the project of seeking emancipation and deterritorialization from banks and states, which lay at the origin of cryptocurrencies, has now been called into question, and the trend seems to be toward a hybridization of debt networks.7

Further reading:

- Aglietta, M. (1988), "L'ambivalence de l'argent," *Revue française d'économie*, 3, p. 87-133.
- Aglietta, M., Orléan, A., ed. (1998), *La monnaie souveraine*, O. Jacob.
- Alary, P., Blanc, J., Desmedt, L., Théret, B. (2016), *Théories françaises de la monnaie*, PUF.
- Banque de France (2018), "L'émergence du Bitcoin et autres crypto-actifs: enjeux, risques et perspectives," *Focus*, 16.
- Bank of International Settlements (2018), "Cryptocurrencies: Looking Beyond the Hype".
- Deleuze, G., Guattari, F. (1973), *L'anti-Œdipe, capitalisme et schizophrénie*, Minuit.
- Desmedt L., Lakomski-Laguerre O. (2015), "L'alternative monétaire Bitcoin: une perspective institutionnaliste," *Revue de la Régulation*, 18.
- Dodd N. (2017), "Utopian Monies: Complementary Currencies, Bitcoin, and the Social Life of Money," in N. Bandelj, F. Wherry, V. Zelizer, eds., *Money Talks, Explaining How Money Really Works,* Princeton University Press, p. 230-247.
- Mackenzie D., Millo Y. (2003) "Construction d'un marché et performation théorique. Sociologie historique d'une bourse de produits dérivés financiers," *Réseaux*, 6/122, p. 15-61.
- Nakamoto S. (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System"
- Nakamoto S. (2009), "Bitcoin Open Source Implementation of P2P Currency," *P2P foundation*.
- Pfister, C. (2017), "Monetary Policy and Digital Currencies: Much Ado about Nothing?," *Banque de France, working paper* 642.
- Riva, A. (2010), "Quand Proudhon critiquait la spéculation," *La Vie des Idées*.

[7] In their 1973 book, Deleuze and Guattari explore the idea that capitalism implies a "decoding of flows" and the erasing of earlier codes (feudalism, despotism). Besides deterritorialization, they mention the circulation of "blocks of debt" that are "open and finite" (see p. 227). Could this be blockchain? Montreal's SenseLab has sought to revive some of these ideas at present

First published in *laviedesidees.fr*, 3 July 2018.

Translated from the French by Michael Behrent with the support of the French Institute (Institut français).

Published in *booksandideas.net*, 27 December 2018.