The disenchantment of Bitcoin: unveiling the myth of a digital currency

Fiammetta Corradi & Philipp Höfner

Routledge
Taylor & Francis Group

ARTICLE

Check for updates

The disenchantment of Bitcoin: unveiling the myth of a digital currency

Fiammetta Corradi[a] and Philipp Höfner[b]

[a]Department of Economics and Management, University of Pavia, Pavia, Italy; [b]Faculty of Business and Economic, Technical University of Dresden, Dresden, Germany

ABSTRACT

Bitcoin and its peculiar, decentralized transaction system, have already ignited interest by professional and retail traders in search for profits and by economists and legal experts, looking for possible regulation to contain illegal uses. We instead examine the unexpected and ongoing success of Bitcoin from a sociological perspective, first questioning its unusual legitimation system, backed by the so called 'blockchain technology', instead of by governmental authorities. Then we collect data and elements to reconstruct Bitcoin's history as a cryptocurrency, starting from the mysterious story surrounding its birth. We then follow its spread and development through social networks and words of mouth, together with its sudden booms and bursts, finally to suggest that both users and institutional regulators should be aware of the risks of Bitcoin and of its alleged power to challenge our very notion of money.

1. Introduction

'Blessed indeed will be the day when it will no longer be from the benevolence of the government that we expect good money but from the regard of the banks for their own interest' (Hayek, 1990, p. 131; first edition 1976). Echoing A. Smith's famous words, so wrote F.A. Hayek more than 40 years ago, arguing for an open competition among multiple currencies, issued by private banks, finally able to provide 'good money' to be 'relied on'.

The birth and quick global success of Bitcoin protocol and bitcoins since 2009 (usually written singular with uppercase B to point to the protocol and plural lowercase to name the currency, shortened to BTC), led some researchers in the field to rename bitcoin 'Hayek Money' and to state that 'Hayek would be happy to know that this blessed day has indeed arrived' (Ametrano, 2016, p. 9). Greeted with unconditioned enthusiasm by libertarians and, alternatively, with great suspect and aversion by other economists (just to name one, Krugman defined it as 'Evil' (2013), the so-called Bitcoin revolution still awaits a sociological interpretation, one able to question critically its alternative solution to the problem of trust in money, and to highlight the roots, potentialities and risks of its apparently never-ending capacity to break new records (the US/BTC ratio skyrocketed in

2017, breaking the $8,000 level in late November, with an yearly increase of more than 750%).

Accordingly, we first reconstruct Bitcoin's development, trying to disentangle the complex mix of history and myth surrounding its birth and its quick transformation from a low-cost transaction means of payment to a tradable asset (§ 2). Then, we turn to the constitutive and characterizing features of Bitcoin as a peculiar system, analyzing its distinctive elements, rules and functioning (including the main technical innovation it implements, namely the 'blockchain') and examining its uncertain classification as a currency, to focus on the 'mystery' of an apparently trustless form of money (§ 3). Finally, we argue that, despite its presumed novelty in the landscape of digital and crypto currencies, and its innovative solution to the double-spending problem, Bitcoin is not different from other traditional financial assets, being it liable to the potentially disruptive powers of 'animal spirits' and the perverse effects of self-fulfilling prophecies (§ 4).

2. Bitcoin between history and myth

2.1. History and ideology

In September 2017, Yale Economics Professor Robert Shiller, Noble prize winner, declared in an interview that one of the best examples of irrational exuberances is Bitcoin, the most important cryptocurrency worldwide. And he significantly added: 'big things happen if someone invents the right story and promulgates it'(Detrixhe, 2017). Much of the fascination of Bitcoin enroots rightly in the mix of history and myth that have enveloped its origin as well as its evolution.

The story and the myth both begin in 2008, in the middle of maybe the deepest crisis that ever hit the modern financial system (Stiglitz, 2010), when a nine-page-long white paper, written by a man with the mysterious pseudonym of Satoshi Nakamoto, appears in the wide space of the internet. The title of the white paper is 'Bitcoin: a peer-to-peer electronic cash system' and its main, declared purpose is to introduce a new digital payment system that does not rely on a trusted third party. In such a new system, any transaction is directly processed between sending and receiving parties and verified by an open and decentralized peer-to-peer computer network, a brand-new solution to the so-called double-spending problem (more details in § 3.1). In this way, with somehow a perfect timing, Bitcoin openly attacks the fiat banking system on its weakest point during the financial crisis: on trust.

Many empirical studies have satisfactorily shown that general trust in private and public banks heavily eroded after the bankruptcy of Lehman Brothers and the following developments within the global financial system (Gurría, 2009; Roth, 2009, p. 204). Still nowadays trust has not regained pre-crisis levels (Cremer, 2015) and more and more people seem to believe that the actual monetary system is no longer sustainable (see Edelman Trust Barometer at www.edelman.com).[1] The collapse of international banks and the following state intervention with taxpayers' money have supported the idea that banks have become 'too big' and too interconnected to fail (Sorkin, 2009). Moreover, central banks got into the focus of critics when starting to use unorthodox approaches to boost the economy. Quantitative easing, negative interest rates and dubious bond purchase program by the ECB (European Central Bank) led to a further decline in investors'

confidence, through to the questioning of their ability to regulate the monetary system and, ultimately, even the democratic legitimization of central banks (Corradi, 2012b; Gros & Roth, 2009).

Within this landscape, Nakamoto's white paper settled the ground for a positive acceptance of a new currency, promising to do without financial intermediates and a centralized power. However, such acceptance was not immediate (BTC prices did not rise immediately; rather, for months they were worth only a few cents, as shown in Figure 4) and the large public took a while to realize the potential of Bitcoin technology and its eventual application as a new money paradigm.

Moreover, probably against the founder's best intentions, the early usages of the new currency for payments were mostly criminal.[2] In particular, the decentralized bitcoin payment system in combination with the Tor browser (which gives users secure access to the 'dark net'), enhanced the possibility for a new business model for trading online illegal products like drugs, child pornography, weapons and fake passports.

Since 2011, more clouds of a criminal fame crowded over Bitcoin, due to its coupling with the website 'Silk Road' and with WikiLeaks.[3] Right in those years the website 'Silk Road' was dominating the field, thanks to an internal rating system, similar to the ones implemented by legal commercial sites like Amazon or eBay (Christin, 2012, p. 20; Van Hout & Bingham, 2014, p. 186). Significantly, its main administrator named himself 'Dread Pirate Roberts' (DPR), a pseudonym recalling the mysterious hero of the novel *The Princess Bride*, by William Goldman (1973).[4] Thanks to an FBI investigation,[5] it emerged in 2014 that behind DPR was the 24-year-old engineer Ross Ulbricht, who was inspired by the libertarian ideas of the Austrian school.[6] In addition, when Ulbricht was imprisoned, CNN reported that two FBI Agents involved in the investigation had stolen huge amounts of bitcoins from the Silk Road account for their own use (Perez, 2015).

After a tentative implementation in the realm of computer games,[7] the Bitcoin community changed strategy to ennoble its status, image and prestige, stressing its debts to the Austrian school and the libertarian ideas of C. Menger, L. von Mises and especially F.A. von Hayek. Often quoted was, for instance, a passage from the *Denationalization of Money* by Hayek (1990, p. 131): 'We have always had bad money because private enterprise was not permitted to give us a better one.' In the imaginary scenario of freely competing private currencies portrayed by Hayek, Bitcoin presented itself as the perfect tool (promising security, anonymity and speed) to finally overcome the limits of any fiat currency, namely government monopoly, which according to Hayek (1990, p. 28) 'has the defects of all monopolies: one must use their product even if it is unsatisfactory, and, above all, it prevents the discovery of better methods of satisfying a need for which a monopolist has no incentive'.

However, compared to Hayek's provocative proposal, Bitcoin moved a step even further, managing to do without the intermediation of banks and of any other formally institutionalized agency in office of issuing the currency and controlling its supply. Supported by such theoretical grounding, the Bitcoin community depicted itself as 'socially useful and valuable'[8] and it surfed the 2008 financial crisis, to side against the political and financial establishment and to foster the construction of a supposedly more open and free society.[9] Not without reason the most important property of the bitcoin ideology seems to be the creation of an unrestrained censorship resistant network.

Matching some of the claims of the 'Occupy Wall Street' movement,[10] Bitcoin also encoded and spread the values of the cypherpunk culture,[11] particularly the endorsement of cryptography, the promotion of open source software and the defense of digital privacy through anonymity.

In the construction and unfolding of the myth of Bitcoin, though, a key role was definitely played by the mysterious character of Satoshi Nakamoto, the Bitcoin's founding father.

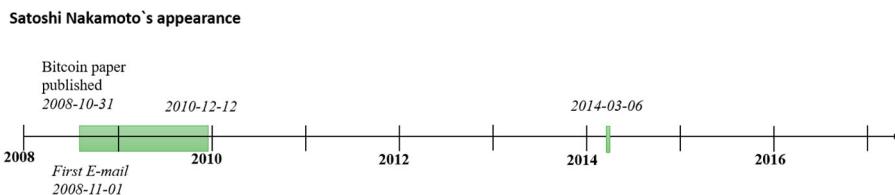## 2.2. The heroization of Satoshi Nakamoto

Since the very beginning of Bitcoin's history, its putative founder, Satoshi Nakamoto, was enveloped in a halo of mystery, stimulating people's phantasy and fostering speculations by the community. His suddenly coming from nowhere to provide people with the bitcoin technology and equally sudden disappearance framed his character by analogy with a prophet or a mythological hero (for instance, as a contemporary Prometheus donating fire to humankind).

Figure 1 shows in detail the attested online activity by Nakamoto.

As one can see, after 12 December 2010, Nakamoto remained silent until 6 March 2014, when the media reported they have found the creator of Bitcoin: a man with the name Dorian Nakamoto, whose former name was Satoshi. Thereupon Nakamoto's P2P account published a post: 'I am not Dorian Nakamoto.' Only weeks later the strong suspicion arose that the account had been hacked (see Bitcoin Forum, http://bitcointalk.org) and that the post's authorship was fake. Some observers have even claimed that, although Nakamoto owns about one million bitcoins, his main interest is to watch and see how society figures out how to deal with his innovation (Lerner, 2013).

Certainly, other elements contributed to the mythologization of Nakamoto and to his cult: the choice of a pseudonym; the publication of his brief, seminal and somehow cryptic white paper (hyperbolically regarded by somebody as an 'holy scripture'); the prophetic tone of some of his statements and even the name chosen for the first block in the Bitcoin blockchain, christened 'Genesis Block'.

The presumed image of Satoshi Nakamoto served also to another purpose: to re-materialize – at least to some extent – Bitcoin as a currency, providing it with some visual support, to overcome its intrinsic 'invisibility'. Instead of George Washington's face, bitcoins in fact display Nakamoto's presumed picture, and the web is rife of bitcoins shining like gold and emulating the dollar sign, substituting the lined uppercase 'S' with the 'B'. Recently, even music on the online platform YouTube supports Bitcoin in its 'phygital' (physical and digital) existence.

Figure 1. Online activity of Satoshi Nakamoto. Source: Re-elaboration from http://satoshi.nakamotoinstitute.org/

3. The mystery of a trustless currency

Setting aside the mythologization process of Nakamoto and other 'soft' devices enforcing and enriching its founding 'meme',[12] a greater and deeper mystery lingers around Bitcoin: how come that so many people trust and trade an apparently unwarranted type of money. We claim in this paragraph that Bitcoin has so far managed to successfully substitute trust in money with trust in technology and in a fully automatized system of rules and procedures, thanks to the innovative combination of a peer-to-peer network system with the so-called 'blockchain technology'.

3.1. The peer-to-peer network and the blockchain

The almost forgotten *Philosophie des Geldes* (1900) by George Simmel reminds us that, since the passage from commodity currency to fiat currency, trust in money is deeply embedded in the reciprocally beneficial 'double bind' between money and the political power of the national state. The relatively young Euro currency, despite the strong influence that national states still retain on it, already hints at a break of continuity with such tradition: for the first time in history, the Old Continent experiences the challenge of a currency issued and controlled by a central, formally independent bank (the European Central Bank was significantly the main addressee of public distrust during the latest financial crisis, for more details, see Corradi, 2012a). Within this tradition, Bitcoin presents itself as an absolute revolution, even though it is not the first digital currency (for an exhaustive overview see Tasca, 2015), nor the first or the last currency based on cryptography.[13]

As explained by S. Nakamoto in his 'White Paper' (2008), its major novelty lies in the combination of a decentralized peer-to-peer (P2P) network system[14] with the so-called 'blockchain' technology: together, they provide a new solution to the old, so-called 'double-spending' problem, namely, the possibility of re-using the same amount of money twice (or even more times), while processing a transaction. While the traditional way of solving such problem implies the existence of a third party in charge of checking each transaction's uniqueness (i.e. banks or other financial intermediaries), Bitcoin uses a distributed network where the nodes are not hierarchically disposed as client and server, but where each node can communicate directly with any other node in the net (for more details: Böhme, Christin, Edelman, & Moore, 2015). In this way, control over double-spending is assigned to the users themselves rather than to a centralized authority (with a significant reduction in transaction fees). Its condition of capacity is the blockchain technology, through which each transaction is computationally recorded and *made public*.

The public ledger is kept thanks to some of the nodes/users, named 'miners'. The miners, receiving the (low) transactions fees, check the validity of transactions in bitcoins providing the computational power of their pc to the network and assembling the transactions occurred in the last 10 minutes in a file termed 'block'. To warrant the validity of each block, the system uses a cryptographic protocol known as 'proof-of-work' (inspired to the Hashcash of Adam Back), that makes the validation of a block a mathematical problem whose solution implies growing degrees of difficulty.[15] Once a node has checked a block, the solution is sent to anybody else and he/she receives a certain number of bitcoins as payback (currently 12.5 BTC); in this way, the blockchain is progressively built through network cooperation and, finally, socially shared.[16]

Mining conveys intrinsic value to bitcoins (since computational power is costly), and at the same time it makes defection to the system *irrational* (a user should own 51% of the overall system computational power to validate a fake transaction block!). In passing, the lexical choice adopted by the community fits with the analogy between bitcoins and gold. As 'real' miners dug for gold since the Californian Gold Rush in the seventeenth century (1840s), with growing efforts and decreasing profits, so 'digital' miners dig for bitcoins, with growing efforts and decreasing profits, because Bitcoin, exactly like gold is a 'limited commodity': its quantity is in fact fixed at 21 million (which seems to promise a deflationary course).

These are, in a nutshell, the technical basics warranting trust in Bitcoin. Since many users – apart from miners – are not familiar with such technicalities, trust in Bitcoin remains for many a leap of faith. Hence, it seems reasonable to state that within the progressive dematerialization process that money has witnessed over time, from commodity money, to fiat money until its digital form – some kind of trust is still necessary for money affirmation and diffusion as means of exchange and as store of value. This remark is once again coherent with George Simmel's pioneering insight about the importance of trust as the main non-economic condition of money. Over time, however, the reference-content of trust has significantly changed: we have passed from trust in the intrinsic value of coins and notes, to trust in the issuing centralized authority (being it the State or central banks) to trust in the technology and in the *automatic* functioning of a system of rules and procedures shared by the community to control transactions. One of the crucial functions of money, however, has gone missing with Bitcoin, as the next paragraph will argue.

3.2. The anomaly of Bitcoin as money

While the academic community and the American Congress debated over the legal status of Bitcoin (see Barber, Boyen, Shi, & Uzun, 2013; Capaccioli, 2015; Grinberg, 2011; Lo, 2017), the EBC, in a report commissioned in 2012 for prospective regulative purposes, classified Bitcoin as a means of payment of the 'third virtual type'. Within the range of digital and crypto currencies, in fact, the exchangeability between virtual and real money is chosen as effective *criterium divisionis*: accordingly, Bitcoin is classified (together with the Linden Dollars circulating in Second Life) among the currencies characterized by a bidirectional flow.[17]

All these classificatory efforts, however, focus on the function of money as means of exchange, leaving undiscussed the other fundamental ones – unit of measure, store of value and credit. Bitcoin can perform well enough as yardstick of measure, being divisible in very small units (the smallest token is called 'Satoshi', and it is worth 0.00000001 bitcoin). It can also be an interesting means to store capital through hoarding strategies, since the ceiling of 21 million units settled by principle to its supply should lead to a deflationary process (London, 2014). Consequently, the simple fact of owning bitcoins should provide increased value over time (it must be noted, however, that the accumulation of bitcoins in a digital wallet is not rewarded with interest). Data support that Bitcoin has so far ignited interest by asset 'keepers', fostering hoarding strategies. Already in 2013, in fact, a study proved that an enormous share of bitcoins does not circulate in the market (Ron & Shamir, 2013). According to such source, the 609,270 addresses that just receive

bitcoins, without sending any, total about 78% of the overall available amount. In addition, more than 76.5% of this percentage are classified as 'old coins', received at least three months before the reference date.

In any case, the same upper limit fixed to its quantity, also makes Bitcoin constitutively unfit to perform the credit function, one that notably plays a key role in the modern and contemporary economy. Hanley (2013) has already developed a harsh critique to Bitcoin, starting right from the fact that new money cannot be created through lending bitcoins: in fact, they are, by definition, not duplicable.[18] By the by, who would rationally borrow bitcoins, where this currency is programmed to increase its value over time?

The fact that Bitcoin can't perform the credit function, however, does not impede its use as a tradable and speculative asset, neither saves it from the usual, often dramatic effects that trust and distrust excesses often have on the financial system.

4. Impact of breaking news on Bitcoin

As any bitcoins trader knows, bitcoins are tradable 24 hours, 7/7 days: exactly as the other currencies traded in the Forex exchange. Probably fewer remind, however, that bitcoins are traded in competing OTC (Over the Counter) markets, typically much less supervised and controlled than the other regulated markets. The complete absence of third part 'gate-keepers',[19] like the SEC in the USA (or the CONSOB in Italy), as well as the inexistence of clearing houses containing, even though not nullifying, eventual insolvencies (for instance the Depository Trust and Clearing corporation), add risks to the intrinsically risky practice of trading assets for speculative purposes.

In the history of Bitcoin, so far, the major flash crash in bitcoin prices was due to the clamours failure of Mt. Gox exchange (set in Tokyo), in the first months of 2014. Notwithstanding the fact that Mt. Gox had a sort of monopoly over bitcoins, with more than 90% of the traded volumes, the BTC/USD ratio (as well as the Coindesk B.P.I.)[20] managed to recover quickly, to start rising again since 2015 (see Figure 2).[21]

Figure 2. Ratio BTC/USD since 2009. Source: https://blockchain.info/de/charts/market-price?timespan=all

From the same chart, the reader may also have a taste of the incredible appreciation bitcoins have witnessed in less than 10 years (from $0.0769 in the first trading day until over $8,000 in mid-November 2017!).[22]

Especially in 2017, when the BTC/USD ratio has gained more than 750%, 'prophets of doom' have multiplied, warning that Bitcoin could be a speculative bubble. Some, echoing Shiller's study about irrational exuberances, have recalled the famous tulip-mania phenomenon which took place in Europe in the seventeenth century; others have labelled Bitcoin a Ponzi scheme.[23]

Although we have different reasons for considering both these analogies inappropriate,[24] it is nonetheless true that there are elements in its fast and exponential appreciation that should suggest prudence.

An aspect that deserves attention– is Bitcoin mid-term 'resilience' to negative news, that is, its ability to recover very quickly from any bad breaking news affecting it and its ability to maintain – so far – an upward technical trend, keeping breaking brand new records (see Figure 3).

In fact, while there is a growing technical literature studying the Bitcoin fair value and price volatility (for sophisticated technical analyses see Ametrano, 2016; Capoti, Colacchi, & Maggioni, 2015; Simeone, Mancini, & Ianiro, 2014), few checked systematically Bitcoin's reactions to exogenous news – in line with the tradition inaugurated by the pioneering work by Shiller (2000) and fostered by the new sociology of finance (for an overview see Corradi, 2016). One step in this direction was already made in 2014 by a website – cryptocurrency news – which is displayed the chart set out in Figure 4.

According to the website cryptocoinsnews, 'Evidence suggests that market participants are *catalyzed into action* by news announcements but that the direction of price movement is mostly unrelated to the actual content of the news and determined by the social mood at the time.'

A closer look at the chart (Figure 4), however, boosts further considerations. On the one hand, it seems that positive, unexpected announcements have on average much greater impact on prices than negative ones, even when the news just 'ventilates' a positive

Figure 3. Technical analysis of BTC/USD ratio from September to November 2017. Source: www.milanofinanza.it
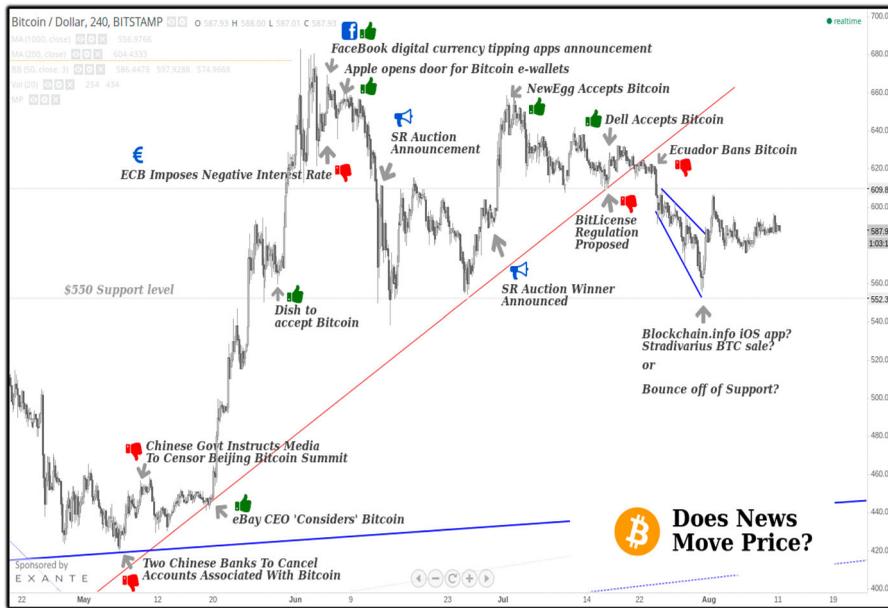
Figure 4. News impact on Bitcoin price. Source: https://www.cryptocoinsnews.com/affects-bitcoin-price/

turn, rather than conveying certainty (look for instance at the news 'eBay Ceo "considers" Bitcoin' and the immediate, subsequent uplift in prices). On the other hand, both positive and negative sudden price moments are often anticipating the actual announcement of expected 'news' (see for instance the downward trend anticipating the news that 'two Chinese banks cancelled accounts associated with bitcoins', or the upward trend anticipating that 'NewEgg accepts bitcoins'). This evidence suggests that bitcoins traders follow, as for many other assets, the old saying that 'buy/sell on the rumors and sell/buy on the news' (a financial declination of the self-fulfilling prophecies).

Longer synoptic time series, matching price movements and news announcements – like the detailed and updated chart available online on 99bitcoins (see https://99bitcoins.com/price-chart-history/) – help deepening and testing the analogy between bitcoins and other assets. If we draw a distinction between *endogenous news* (referring to Bitcoin usage or the community at large) and *exogenous news*, we note that news having direct relevance to Bitcoin generally affects its price more than external (though economic) news.

Moreover, endogenous news seems to be positively correlated with the content of the news itself. So, for instance, the so-called 'halving days' – days in which the planned halving of bitcoins reward for miners occur – are coupled with sensible, positive price variations (28 November 2012 and 9 July 2016). Analogously, the allowance of bitcoins as means of payment within online agencies – or their ban – witnesses coherent price variations (the experience of Mt. Gox is exemplary). Similarly, prices skyrocketed on 1 April 2017, when Japan passed a law promoting Bitcoin as an officially legal currency in the country; and on 13 July 2017, when the first Swiss private bank announced offering their customers a Bitcoin asset management service.

More recently, the announcement of a huge theft in Tether[25] worth about 32 billion USD on November 19, made the asset fall suddenly of about 5.4% (followed by a fast recovery). While most of the previous shocks can be considered external, Bitcoin recently faced a major inner split that ended with the creation of a new bitcoin chain, called Bitcoin Cash. This is the provisional outcome of an ongoing discussion about how to scale the bitcoin network in order to allow a broader adoption. While Bitcoin Cash's supporters want to increase the block size to scale, Bitcoin Core's advocates insist on an outsourced scaling solution. A previous arranged compromise (Segwit2x) failed on 19 November 2017. The divisiveness of the Bitcoin community may have much stronger effects than external factors. From an evolutionary perspective, in fact, the split of the Bitcoin blockchain resembles the creation of a new species. Indeed, one can speak of a 'fratricidal or civil war'. Which chain will survive in the end is yet unpredictable, but competition in general goes in unison with Hayek's free market solution.

The impact of exogenous news is less easy to assess, but it seems in any case content-dependent. Our impression is that Bitcoin price reactions resemble the reactions of many assets traded on regulated markets, even if bitcoin shows – so far – a stronger *resilience* to news that is unexpected or considered as negative by financial investors. Although additional analyses are needed to assess the validity of this conjecture, some significant cases seem to support it. On 9 November 2016, when contrary to any market expectation Donald Trump defeated Hillary Clinton and was elected 45th President of the United States, the established stock markets globally plummet (to rapidly recover afterwards).[26] Bitcoin immediately followed suit, but it quickly recovered in the following hours, to even start an upward trend in the following days.[27] Analogously, in the Fall of 2017, the US–North Korea 'words-conflict' and the alleged international geopolitical tensions impacted less on Bitcoin than on the regulated stock markets, although even there the negative expected reaction was overall contained (probably due to the positive macroeconomic data supporting the economies on both sides of the Atlantic Ocean).

5. Conclusions

The relative novelty of Bitcoin as a currency and as an asset makes any forecast tentative and provisional, calling for deeper and more systematic analyses to assess its future potentialities and risks. Nonetheless, this work has started to build a sociological perspective committed to understand Bitcoin as a 'social fact', as a phenomenon whose past roots and future developments are intrinsically social.

Trying to disentangle Bitcoin history and myth, splitting its mysterious origins and developments in memes, analyzing the 'hard' and 'soft' devices employed to warrant and enhance trust in a constitutively trustless form of money, we have highlighted both Bitcoin's innovative character and revolutionary ambitions as a currency, and its 'social, too social' nature as an asset, volatility, flash crashes and fast recoveries. We have argued that Bitcoin owes much of its success, rather than to economic fundamentals, to mythological narrative, advertising, word of mouth, and other social mechanisms based on emotions (fear of missing out, uncertainty and doubt): the 'animal spirits' – whose power might be far to be unleashed – that so often foster 'irrational exuberances'.

At the same time, we have shown that the success of Bitcoin partly depends on its coherence with the contingent merger of libertarian and anti-establishment ideas we

witness in our time. Our short analysis of the impact of breaking news on Bitcoin prices, in fact, suggests that the resilience against unexpected or negative news could also be interpreted as an effect of Bitcoin's constitutive trust in a censorship resistant technology.

Consequently, we have reached the more general conclusion that, despite any declared purposes and hopes, Bitcoin cannot truly do without some form of trust, as Simmel had already foreseen more than a century ago. Rather, we believe that, within the money dematerialization process, only the *content* of trust has changed over time, being the one bestowed upon Bitcoin mainly trust in technology and in the automatic functioning of a shared system of rules and procedures. However, the ongoing internal competition between Bitcoin Core and Bitcoin Cash (what we considered as a 'civil or fratricidal war'), being a conflict about the fundamental mechanism of blockchain and its scaling, could lead to really unexpected outcomes (probably decided by the market, in the end). Independently from the future evolution of Bitcoin prices, we are confident that the Bitcoin phenomenon is of intrinsic economic and sociological interest, especially when it is conceived as a 'social experiment' with a new form of money, based on a new form of trust.

Notes

1. See Edelman Report 2015 on www.edelman.com. In addition, the 2015 Edelman Trust Barometer shows that 'only 40 percent of the general global population trusts in cyber currency or Bitcoin technology. That makes it the least trusted technology sector, coming in more than 10 points lower than trust in cyber security technology, eCommerce technology or smart home technology': Retrieved from http://www.edelman.com/post/future-bitcoin-lies-trust/ [Accessed 10 March 2015].
2. In outright opposition with such criminal and detrimental usages, a different cryptocurrency based on the Bitcoin protocol was conceived by Effemera Network. Named 'Commoncoin' after a meeting of the network in Milan, the new currency was addressed at the circuit of Italian occupied theaters, at the movements of precarious workers, at the network of social centers. Commoncoin 'aimed to contribute to the invention of an alternative economic system as a form of finance/credit money able to remunerate social cooperation and the work performed by the general intellect' (Terranova & Fumagalli, 2015, p. 153).
3. The connection between Bitcoin and WikiLeaks emerges through some posts published online by Julian Assange and by Satoshi Nakamoto himself. When WikiLeaks was refused donations from banks and other organizations, its founder ventilated the idea of accepting bitcoins as a donation method and communicated his idea in ANA Reddit.com discussion. His proposal encountered some favour, but also harsh resistance, as expressed in this post (5/10/2010): 'The project needs to grow gradually so the software can be strengthened along the way. I make this appeal to WikiLeaks not to try to use Bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage' (Satoshi Nakamoto Institute, satoshi.nakamotoinstitute.org/posts/bitcointalk/523) [Accessed 5 December 2010]. Later Nakamoto stated: 'It would have been nice to get this attention in any other context. Wiki-Leaks has kicked the hornet's nest, and the swarm is headed towards us' (Satoshi Nakamoto Institute, satoshi.nakamotoinstitute.org/quotes/general) [Accessed 11 December 2010]. Assange explained in Reddit.com that Wikileaks stopped bitcoin donations on WikiLeaks, a possibility rehabilitated six months later and still open nowadays.
4. In this novel, the mysterious hero is not one man, but a series of different persons who pass all the name to a chosen successor, once they are wealthy enough to retire.
5. This event impacted strongly on the Bitcoin price. During the Silk Road investigation, a variety of media reports about bitcoins pushed the price per coin up to $1,000 and after the first

bubble of bitcoin busted in 2014, bitcoin vegetated until the end of 2015 at a price around $220. More on bitcoin price variations in § 4.

6. Ulbricht wrote in his LinkedIn page: 'I want use economic theory as a means to abolish the use of coercion and aggression amongst mankind' and 'I am creating an economic simulation to give people a first-hand experience of what it would be like to live in a world without the systemic use of force' (Dewey, 2013).

7. Next to the use in the so called deep net, bitcoin also found entrance into the computer gaming scene. Gamers used bitcoin as payment method for trading virtual products within computer games and on computer games platforms, like Steam, the leading gaming platform developed by the Valve Corporation, which offers digital rights management. Users can purchase games, communicate with other users and store their games. Also starting with this nerdy background was inappropriate for bitcoin to scale.

8. Somebody wrote on an online platform: 'The bitcoin system turns out to be socially useful and valuable, so that node operators feel that they are making a beneficial contribution to the world by their efforts […] In this case it seems to me that simple altruism can suffice to keep the network running properly.' And Nakamoto answered: 'It's very attractive to the libertarian viewpoint if we can explain it properly. I'm better with code than with words' (Satoshi Nakamoto Institute, 'The Quotable Satoshi', http://satoshi.nakamotoinstitute.org/) [Accessed 14 November 2008].

9. On 1 November 2008, a user wrote: 'You will not find a solution to political problems in cryptography.' Nakamoto answered: 'Yes, but we can win a major battle in the arms race and gain a new territory of freedom for several years. Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own' (Satoshi Nakamoto Institute, RE: Bitcoin P2P e-cash paper, http://satoshi.nakamotoinstitute.org/emails/cryptography/4/) [Accessed 7 November 2008].

10. The organization team of 'Occupy Wall Street' accepted donations in bitcoins. The reason was the refusal of PayPal to pass transactions of donors ('Occupy Wall Street Protesters Accepting Donations in Bitcoin: Big Test for the Controversial Virtual Currency', New World Notes, http://nwn.blogs.com/nwn/2011/10/bitcoin-donations-for-occupy-wall-street-feed-the-protest.html) [Accessed 3 October 2011].

11. The online Cypherpunk manifesto reads: 'Privacy is necessary for an open society in an electronical age […] We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence' (http://www.activism.net/cypherpunk/manifesto.html) [Accessed 12 October 2017]. Cypherpunks are strong supporters of open source software and a free and private use of the internet. Moreover, the famous cypherpunk cryptographer Jacob Appelbaum, was the creator of the anonymous Tor internet browser, which in combination with Bitcoin, was the base for illegal online shops.

12. According to the Cambridge Online Dictionary, 'the "meme" is the cultural equivalent of the unit of physical heredity, the gene' (http://dictionary.cambridge.org.it) [Accessed 25 September 2017]. Its specialized usage in informatics, however, hints at an idea, image, video etc. that is spread very quickly on the internet. Notoriously Levi-Strauss already used the term to signal the smallest autonomous unit of a myth, with a coherent meaning.

13. Cryptography is as old as human beings invented rules and keys to hide a message content (Julius Caesar had a passion for it). A revolution in cryptography, however, was to occur only in the twentieth century, when it became asymmetric, through the implementation of a public key to encrypt a message, and a private one, to decrypt it. To increase the reliability and security of an encryption, the Hash function has been developed and finally used to get a digital digest of a message. Cryptography and Hash functions are the basics of any digital signature.

14. 'In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin' (http://www.satoshispeaks.com) as S. Nakamoto wrote in a post (11/02/2009).

15. The difficulty changes automatically every 2016 blocks and has reached skyscrapers levels, such that already in 2013 only enormous pc, as huge as wardrobes, were able to solve them.

Nowadays, even a dedicated, specialized software named ASIC (Application Specific Integrated Circuit), worth some thousand dollars, can mine daily only a small share of bitcoins.

16. So far, Bitcoin has developed coherently with the Metcalfe's law on network expansion, according to which the value of a communication is proportional to the square of the number of connected users of the system (n^2). In other words, the value of networks increases exponentially with additional users, and the same happens to each user's utility.

17. An examples of the first type (money acquirable and usable only within the close community) is the gold of World of Warcraft; examples of the second type (money acquirable from outside but usable only within the community) are Facebook Credits and Microsoft points.

18. In Hanley's (2013, p. 13) words: '[…] creating loans based on bitcoin would require a new entity, the virtual-bitcoin, which would be backed by bitcoin, but not actually be bitcoin, just as gold-backed currency is backed by gold but not actually itself gold. In this virtual-bitcoin scenario, bitcoin banks would keep bitcoin on reserve and redeem the virtual-bitcoin for real bitcoin in transfers, payments, etc. […] To make virtual-bitcoin work would require a central clearinghouse to authorize the transactions, and then bitcoin would have come full circle – implementing the central clearinghouse accounting authority it was created to put an end to.'

19. There is a blooming literature in economics and in sociology dealing with the riddle of controlling the controllers. In the 2008 financial crisis, the main rating agencies such as Moody's and Fitch were under the critical loupe (see e.g. Catino, 2010).

20. The Coindesk Bitcoin Price Index, published by the web www.coindesk.com, synthetizes the prices of the exchanges where bitcoins are traded.

21. It is very interesting to note that right the country in which Mt. Gox was born – Japan – soon recovered from the shock affecting Bitcoin, quickly becoming one of the frontrunners in its promotion and specific regulation. In April, 2017 – in fact – Japan emended a revolutionary law (the Payment Services Act, part of the Banking Act) to define virtual currencies as a legal form of payment, establishing capital requirements for exchanges, cyber security and operational stipulations. On this topic see LaMarsch (2017) and Lo (2017, p. 114).

22. On 29 November 2017, the new record of 10,000 USD has been broken.

23. According to the US Securities and Exchange Commission a Ponzi Scheme is defined as: 'an investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors. Ponzi scheme organizers often solicit new investors by promising to invest funds in opportunities claimed to generate high returns with little or no risk. In many Ponzi schemes, the fraudsters focus on attracting new money to make promised payments to earlier-stage investors and to use for personal expenses, instead of engaging in any legitimate investment activity' (U.S. Securities and Exchange Commission, Ponzi Schemes, What is a Ponzi Scheme? http://www.sec.gov/answers/ponzi.htm) [Accessed 29 October 2017]. For a presentation of historical examples of Ponzi Schemes see also Corradi, 2016, p. 39.

24. The analogy with the Tulip mania is unsound because, in contrast to tulips, bitcoins have utilities for their users (bypassing capital controls, avoiding taxation, reducing transaction costs …), and because tulips, in contrast to bitcoins, had no pre-determined (and known) supply limit. On the other hand, it would be improper to consider bitcoin a Ponzi scheme because it lacks many of the features mentioned in the above definition, like the constitutive role of the hoaxer.

25. A synthetic digital currency that is according to its whitepaper 100% backed by USD. Tether are used by major exchanges to bypass regulations and ease the trading process between crypto currencies. The intention of Tether is to avoid a back shifting of digital currencies into fiat currencies.

26. Japan's Nikkei 225 plunged 5.4% while Hong Kong's Hang Seng index lost 2.2%. The Shanghai Composite index lost 0.6%. Dow futures were down 2.1%, S&P 500 futures were 2.3% lower and Nasdaq futures lost 2.7% at around 6.30 am E.T. On that same day, European markets opened sharply lower before paring its losses. Germany's DAX index was off around 1% after opening down nearly 3%. France's CAC 40 was in positive territory by 0.4% after an earlier decline of 1.5% and Britain's FTSE 100 dropped 0.3%.

27. Further empirical analyses should also test whether Bitcoin and gold really display similar trends, as ventilated by some posts relieved by the bitcoin community, where the hope is shared that bitcoin can become one day a new reserve currency. So far, we can just notice that bitcoin and gold are favorite assets for holding strategies.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Fiammetta Corradi teaches 'Sociology' and 'Economics & Society' at the Department of Economics and Management of the University of Pavia. She is author of many works in the field of the Sociology of Cultural and Communicative Processes and in the Sociology of Finance. Her latest book is *Social Spirits: A New Research Agenda for the Sociology of the Stock Exchange*.

Philipp Höfner is a Master student in economics at the Faculty of Business and Economics of the University of Dreden.

References

Ametrano, F. A. (2016). *Hayek Money: the Cryptocurrency Price Stability Solution*. Retrieved from https://ssrn.com/abstract=2425270 or http://dx.doi.org/10.2139/ssrn.2425270

Barber, S., Boyen, X., Shi, E. … Uzun, E. (2013). Bitter to better. How to make bitcoin a better currency. In A. Keromytis (Ed.) *16th international conference on financial cryptography and data security* (pp. 399–414). Berlin: Springer.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, *29*(2), 213–38.

Capaccioli, S. (2015). *Criptovalute e bitcoin: un'analisi giuridica*. Milano: Giuffré.

Capoti, D., Colacchi, E., & Maggioni, M. (2015). *Bitcoin revolution. La moneta digitale alla conquista del mondo*. Milano: Hoepli.

Catino, M. (2010). Gatekeepers miopi? Aspetti organizzativi nel fallimento dei controlli. *Stato e Mercato*, *89*, 219–253.

Christin, N. (2012). *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*. Pittsburg, PA: Carnegie Mellon University. July 30, 2012, Retrieved from https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf

Corradi, F. (2012a). La fiducia dei cittadini europei in una moneta senza stato. *Sociologia Italiana, AIS Journal of Sociology*, 0, 89–106, ottobre 2012, Milano: EGEA (Università Bocconi).

Corradi, F. (2012b). Mercanti di rischio e restauratori di fiducia: Ricostruire la fiducia sistemica mediante discorsi pubblici. *Rassegna Italiana di Sociologia*, anno *LIII*(1), 113–135.

Corradi, F. (2016). *Social spirits. A new research agenda for the sociology of the stock exchange*. Saarbrücken, German: Lambert Academic Publishing.

Cremer, D. D. (2015). *Why Our Trust in Banks Hasn't Been Restored*, reliesed by Harward Business Review. Retrieved from https://hbr.org/2015/03/why-our-trust-in-banks-hasnt-been-restored

Detrixhe, J. (2017). Robert Shiller wrote the book on bubbles. He says 'the best example right now is Bitcoin'. *Quartz*. Retrieved from https://qz.com/1067557

Dewey, C. (2013). Everything we know about Ross Ulbricht, the outdoorsy libertarian behind Silk Road. *The Washington Post*. Retrieved from https://washingtonpost.com/news/the-switch/wp/2013/10/03/everything-we-know-about-ross-ulbricht-the-outdoorsy-libertarian-behind-sil-road/?utm_term=.6839732dec9a

Grinberg, R. (2011). Bitcoin: An innovative alternative digital currency. *Hastings Science & Technology Law Journal*, 4), Retrieved from https://ssrn.com/abstract=1817857" \t "_blank" https://ssrn.com/abstract=1817857

Gros, D., & Roth, F. (2009). *The crisis and citizens' trust in central banks*. Retrieved from VOX CEPR's Policy Portal, 10 September, Retrieved from http://voxeu.org/article/crisis-and-citizens-trust-central-banks

Gurría, A. (2009). *Responding to the global economic crisis – OECD's role in promoting open markets and job creation*. Lisbon: BIAC Business Roundtable. 21 May 2009, Retrieved from http://www.oecd.org/newsroom/respondingtotheglobaleconomiccrisisoecdsroleinpromotingopenmarketsandjobcreationintroductoryremarks.htm

Hanley, B. P. (2013). *The False Premises and Promises of Bitcoin*, Retrieved from http://axiomaticeconomics.com/False_Premises_Promises_Bitcoin.pdf

Hayek, F. A. (1990). *The denationalization of money: The argument redefined*. first edition 1976. London: The Institute of Economic Affairs

Krugman, P. (2013). *Bitcoin is Evil. The New York Times*. Retrieved from https://krugman.blogs.nytimes.com/2013/12/28/bitcoins-is-evil/

LaMarsch, I. (2017). Bitcoin: What it is, How it works, and why it is giving the world a Run for its money. *Oxford Journal: An International Journal of Business & Economics*, 12 (2), 1–10. http://www.ojbe.org/oj/index.php/journals/article/view/133/115

Lerner, S. D. (2013). The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius. *Bitslog, wordpress*. Retrieved from https://bitslog.wordpress.com/2013/04/2017/the-well-deserved-fortune-of-satoshi-nakamoto/

Lo, B. (2017). Fatal fragments: The effect of money transmission regulation on payments innovations. *Yale Journal of Law and Economics*, *18*(1), Article 4. Retrieved from http://digitalcommons.law.yale.edu/yjolt/vol18/iss1/4

London, R. A. (2014). Bitcoin's deflation problem. *The Economist*. Retrieved from https://www.economist.com/blogs/freeexchange/2014/04/money?fsrc=rss

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

Perez, E. (2015). Two former federal agents charged with stealing Bitcoin during Silk Road probe. *CNN*. Retrieved from edition.cnn.com/2015/03/30/politics/federal-agents-charged-with-stealing-bitcoin/index.html

Ron, D., & Shamir, A. (2013). Quantitative analysis of the full Bitcoin transaction graph. In *Financial cryptography and data security, volume 7859 of lecture notes in computer science* (pp. 6–24). Berlin: Springer.

Roth, F. (2009). The effect of the financial crisis on systemic trust. *Intereconomics: Review of European Economic Policy*, *44*(4), 203–208.

Shiller, R. J. (2000). *Irrational exuberance*. Princeton: Princeton University Press.

Simeone, A., Mancini, D., & Ianiro, A. (2014). *Bitcoin guida all'uso. Cos'è, come funziona, vantaggi e rischi*, Exeo, Economia 2.0, Economia, Mercati e Finanza. Retrieved from http://www.exeo.it/Data/Files/HtmlEditor_Files/file/PUBLISHING/EBOOKS/2014/SIMEONE/BITCOIN-guida-sampler.pd

Simmel, G. (1900). *Die Philosophie des Geldes*. Berlin: Duncker & Humbolt Verlag.

Sorkin, A. R. (2009). *Too Big to fail. The inside story of How wall street and Washington fought to save the financial system – and themselves*. New York: Viking.

Stiglitz, E. J. (2010). *Freefall. America, free markets and the sinking of world economy*. New York: Norton.

Tasca, P. (2015). *Digital Currencies: Principles, Trends, Opportunities, and Risks*, UCL, Centre for Blockchain Technology, (September 7, 2015). Available at SSRN: https://ssrn.com/abstract=2657598 or http://dx.doi.org/10.2139/ssrn.2657598

Terranova, T., & Fumagalli, A. (2015). Financial capital and the money of The common: The case of commoncoin. In G. Lovink, N. Tkacz, & P. De Vries (Eds.), *Moneylab reader: An intervention in digital economy* (pp. 150–160). Chennai: Institute of Network Cultures.

Van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk road, the online revolution in drug trading. *International Journal of Drug Policy*, *25*(2) March, 183–189.