Examining the writings of Satoshi Nakamoto:
A Monetary Analysis of the Bitcoin Protocol

Christophe Depoortère[1]

This paper considers the design of the Bitcoin protocol from a monetary perspective. To this end, it relies heavily on the publications of the creator(s) of Bitcoin, Satoshi Nakamoto, on different mailing lists and forums. It first expounds the political and economic motives which led Nakamoto to build an electronic system of payment based on "proof" rather than on "trust". Then, it considers the predetermined character of the issue of bitcoins and support the view that one consequence of this issuing rule is that the bitcoin has no monetary standard-even understood in a broad sense. Finally, it deals with the concept of "synthetic commodity money" and the widespread comparison of bitcoin to the Iraqi Swiss dinar. The notion of monetary standard considered as a measure of the value of money is then used to distinguish these two currencies.

Keywords: Satoshi Nakamoto, Bitcoin, monetary system, synthetic commodity money, standard of money.
JEL classification: B 29, E42, E 50.

1. Introduction

On 31 October 2008, one or more people, acting under the pseudonym of Satoshi Nakamoto, sent an e-mail entitled "Bitcoin P2P e-cash paper" to the "Cryptography Mailing List" of Metzdowd.com. This e-mail announced: "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party" (Cryptography Mailing List, 2008-10-31). Then, Nakamoto listed the main properties of the system and furnished a link to the article: "Bitcoin: A Peer-to-Peer Electronic Cash System". This article is now known as the "Bitcoin white paper"[2]. Following this e-mail, an electronic correspondence took place between Nakamoto and the members of "The Cryptography Mailing List". It lasted till 25

[1] CEMOI, University of Reunion Island

[2] A pre-release draft of this paper was entitled "Electronic Cash without a trusted Third Party" (Nakamoto 2008a). On 22 August 2008, Nakamoto sent it privately to Wei Dai, a computer engineer known for his contributions to cryptography and cryptocurrencies. In 1998, Dai had conceptualised B-Money, an anonymous, distributed electronic cash system (see Dai 1998).

January 2009. Among the members of the list was Hal Finney[3] who supported the project and with whom Nakamoto later exchanged privately. Finney would become an important figure of the development of Bitcoin. Another mailing list was created by Nakamoto on 10 December 2008 on SourceForge: the "Bitcoin List". This list remained active till 13 December 2010.

The bitcoin network was launched on 3 January 2009 with Nakamoto generating the "genesis block", viz. the first block of transaction. This block included the following text as a satirical timestamp: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks". It referred to a headline in *The Times* newspaper published the same day. A 10 bitcoins test transaction occurred nine days later between Nakamoto and Finney.

On 11 February 2009, Nakamoto announced the creation of Bitcoin publicly on the P2P Foundation forums and started exchanging messages with the members of these forums. Finally, on 22 November 2009, Nakamoto opened a new "Bitcoin Forum" usually known as "Bitcointalk". After about one year and more than 500 posts on this forum, Nakamoto announced he retired from the project and ventured "into more complex ideas" (Bitcointalk, 2009-2010, 2010-12-12). He left the responsibility of developing the code and network to a thriving group of volunteers. Four months later, Nakamoto wrote to Mike Hearn[4], that he had "moved on to other things" and that the project was "in good hands" (Nakamoto,2009-2011, 2011-04-23).

After December 2010, only a few messages were posted from Nakamoto's accounts. The first one followed a 2014 article by Newsweek, fingering a Japanese-American man in California named Dorian S. Nakamoto as the inventor of Bitcoin. A denial from Satoshi Nakamoto's account was published on 7 March 2014 on a forum of the P2P Foundation: "I am not Dorian Nakamoto" (P2P Foundation, 2014-03-07). More recently, on 24 December 2021, Nakamoto's account announced on the same forum: "After 13 years of decentralized payment systems evolution we came where we are now, the NFT epoch" (P2P Foundation, 2021-12-24). The message also offered NFT for sale. It is likely that Nakamoto was not the genuine author of this message but that his profile on the P2P Foundation forum had been forced, as it happened with his main e-mail address in September 2014[5].

[3] Hal Finney (1956-2014) was an American software developer who helped Nakamoto early on with the code and became an early adopter of Bitcoin. Finney was interested for long in digital cash and had proposed in 2004 a digital currency system: Reusable Proofs of Work (RPOW). In 2009, Finney was diagnosed with amyotrophic lateral sclerosis. He died in Phoenix, Arizona, on 28 August 2014. On Finney, see Brunton, 2019, pp.154-8.

[4] Mike Hearn was an early Bitcoin developer (2011-2016). In 2014, he left his post of senior software engineer at Google to devote himself entirely to the development of Bitcoin. He quit Bitcoin in January 2016 with a highly controversial blog post reading: "But despite knowing that Bitcoin could fail all along, the now inescapable conclusion that it *has* failed still saddens me greatly. The fundamentals are broken and whatever happens to the price in the short-term, the long-term trend should probably be downwards. I will no longer be taking part in Bitcoin development and have sold all my coins" (Hearn, 2016).

[5] On 8 September, the following message was sent on a P2P Foundation forum from Nakamoto's email address satoshin@gmw.com: "Dear Satoshi. Your dox, passwords and IP addresses are being

The e-mails and posts sent by Nakamoto on the different mailing lists and forums, as well as his private e-correspondence, deal mainly with technical issues connected to Bitcoin protocol and related specifications. They do also include considerations on Banks, money and more broadly, political economy. The "early" correspondence, going from October 2008 till February 2009, provides in particular a good view of Nakamoto's genuine project, and of the distinctive features of bitcoin considered as a currency. It is on these writings[6] and on the Bitcoin white paper, that the present article will mainly rely to propose a monetary analysis of the Bitcoin Protocol.

Section 2 expounds the motives which led Nakamoto to build an electronic system of payment based on "proof" rather than on "trust". It also recalls the political and economic benefits that Nakamoto saw in Bitcoin, compared to traditional monetary systems. Section 3 considers the predetermined character of the issue of bitcoins and support the view that one consequence of this issuing rule is that the bitcoin has no monetary standard-even understood in a broad sense. Section 4 compares bitcoin with the Iraqi Swiss dinar-a "synthetic commodity money" with which it regularly associated- and introduces the notion of standard of money as a measure of the value of money to distinguishes these two currencies. The paper concludes on the emergence of stablecoins as a consequence of the lack of monetary standard in the Bitcoin protocol.

2. Bitcoin: an electronic cash system without a third party.

Much has been written about whether bitcoin is a currency or not, and if not, which asset class it most closely resembles[7]. However, while there are some debates about what bitcoin really is, there is much less doubt about what Nakamoto intended bitcoin to be. Indeed, in the white paper, the inventor of Bitcoin introduced it as an "electronic cash system" which would "allow online payments" (Nakamoto, 2008b, p. 1). Later on, he described bitcoin as an "e-currency" (P2P Foundation, 2009-02-15), a "cryptocurrency" or a "digital currency" (Bitcoin List, 2010-07-06). Thus, as Luther stated, "bitcoin was primarily intended and widely understood to be used as a currency" (2019, p. 199).

sold on the darknet. Apparently you didn't configure Tor properly and your IP leaked when you used your email account sometime in 2010. You are not safe. You need to get out of where you are as soon as possible before these people harm you. Thank you for inventing Bitcoin" (Cointelegraph, 2014).

[6] Researchers interested in Bitcoin appear to have made relatively little use of these writings. Among those who used it are Maurer, Nelms and Swartz, 2013-in a paper investigating the semiotics of Bitcoin.

[7] On the issue of whether bitcoin should be considered a currency or not, see Glaser, Haferkorn, Siering, Weber and Zimmermann, 2014; Yermack, 2015; Bouoiyour and Selmi, 2015; Desmedt and Lakomski-Laguerre, 2015, pp. 5-8 and 2021, pp. 106-7; Ammous, 2018; Baur, Hong and Lee, 2018; Söderberg, 2018; Orléan, 2019, pp. 53-6; Hazlett and Luther, 2020.
On the type of asset bitcoin most closely resemble, see: Dyhrberg, 2016a and 2016b; Baur, Dimpfl, and Kuck, 2018; Corbet, Larkin, Lucey, Meegan and Yarovaya, 2018; Klein, Thu and Walther, 2018; Bouri, Kristoufek, Lucey, Roubaud and Shahzad, 2019; Smales, 2019.

Considered as a currency, an originality of Bitcoin lies in the fact that it does not rely on any central authority[8]. As Nakamoto made it clear, the technical challenge of Bitcoin consisted in preventing the problem of double spending[9] without the intervention of a trusted third party:

> a common solution [to this problem] is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank (Nakamoto, 2008b, p. 2).

Nakamoto solved the double spending problem by "using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions." (Nakamoto, 2008b, p. 1)[10]. This distinguished Bitcoins from former attempts to build digital cash systems such as DigiCash, a project developed in the 1990's by David Chaum[11]. Nakamoto stated:

> after more than a decade of failed Trusted Third Party based systems (Digicash, etc), [people interested in Electronic currency and cryptography] see it as a lost cause. I hope they can make the distinction that this is the first time I know of that we're trying a non-trust-based system (Cryptography Mailing List, 2009-01-16).

In his White paper, Nakamoto outlined some of the advantages he saw in a system based on cryptographic proof rather than on trust[12]. His arguments were essentially about 1) the possibility of carrying out online transactions that would be non-reversible and 2) the reduction of transaction costs that such a possibility would allow. The disappearance of these transaction costs should have made it possible to carry out small transactions that were currently impossible:

[8] For an overview of Bitcoin's design principles and properties, see Weber, 2016; Böhme, Christin, Edelman and Moore, 2015; Dwyer, 2015, pp. 82-6.

[9] The double spending problem lies in the fact that crypto currencies consist of a digital file that can be duplicated. There is thus the possibility that the same single digital coin be spent more than once.

[10] As Nakamoto noted, this solution supposes that no malicious user has 51% or more of the computing power of the Bitcoin network (Nakamoto, 2008b, p. 1).

[11] David Lee Chaum is an American computer scientist and cryptographer born in 1955. In 1989, he founded DigiCash, an electronic cash company. In 1995, his Company created the first digital currency: "eCash". Ecash preserved users' anonymity but required banks to act as trusted third parties. DigiCash declared bankruptcy in 1998. On Ecash, see Brunton, 2019, pp. 53-61. On the various attempts prior to Bitcoin to create a secure and untraceable currency, see Dodd, 2014, pp. 362-4; Desmedt and Lakomski-Laguerre, 2020, pp. 145-6. For a more general view of the history of cryptocurrency, see Brunton 2019.

[12] For a critical view of Bitcoin as a "trust free" money, see Maurer, Nelms and Swartz, 2013; Maurer, Nelms, Swartz, and Mainwaring, 2018, pp. 8-12, and Dodd, 2017.

> Commerce on the Internet […] suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party (Nakamoto, 2008b, p. 1).

In the White paper, Nakamoto also addressed the issue of privacy. He merely pointed out the differences between the Bitcoin protocol and the traditional banking system in the way this issue was handled. However, he did not attempt to point out any advantages of the former over the latter, nor did he claim originality in the way the Bitcoin protocol ensured confidentiality:

> The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were (Nakamoto, 2008b, p. 6).

The tone adopted by Nakamoto when explaining his motives for creating Bitcoin, on the various discussion forums and mailing lists in which he participated, appeared sometimes significantly different from that of the white paper. In these discussions, Nakamoto first developed the applications he contemplated for Bitcoin in the field of micropayments:

> It could get started in a narrow niche like reward points, donation tokens, currency for a game or micropayments for adult sites. Initially it can be used in proof-of-work applications for services that could almost be free but not quite.
> It can already be used for pay-to-send e-mail. […] If someone famous is getting more e-mail than they can read, but would still like to have a way for fans to contact them, they could set up Bitcoin and give out the IP address on their website. 'Send X bitcoins to my priority hotline at this IP and I'll read the message personally' (Cryptography Mailing List, 2009-01-16)[13].

[13] See also Nakamoto 2009, 2009-01-15.

Some weeks later, in the post introducing Bitcoin on the P2P Foundation forums, Nakamoto appeared more offensive against the trust-based model. In addition to bank charges making micropayments impossible, Nakamoto evoked the depreciation of currencies due to central bank's accommodating policies; speculative bubbles originating in expansions of credit by commercial banks which disconnected their issue from their reserves; flaws in the banks' security systems-putting depositors at risk of having their accounts emptied-; and violations of bank confidentiality:

> 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. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible. […] Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers[14] (P2P Foundation, 2009-02-11).

The charge against centralised monetary institutions, associated to overissue and depreciation of money, was repeated in July 2010 when version 0.3 of Bitcoin was announced. At this occasion, Nakamoto described Bitcoin as escaping "the arbitrary inflation risk of centrally managed currencies!" (Bitcoin List, 2010-07-06).

Finally, in a post on the Cryptography mailing list, Nakamoto expressed the opinion that pear to pear networks, such as Bitcoin, was a good answer to the interference of governments and could advance individual freedom-at least for a moment. The reason was that these networks were much less vulnerable to Government attacks than centralised systems:

> 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 (Cryptography Mailing List, 2008-11-06)[15].

[14] Nakamoto added: "A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. […] It's time we had the same thing for money" (P2P Foundation, 2009-02-11).

[15] Nakamoto had probably in mind the US Government intervention against the digital gold currency e-gold. E-gold was a monetary payment system founded by Douglas Jackson in 1996. Jackson was an oncologist interested in Austrian economics. E-gold allowed users to transfer digital tokens 100% backed and convertible into gold. In December 2005, FBI agents raided E-gold offices and in April 2007, Jackson was accused, by federal prosecutors, of money laundering and of illegal money transmitting. Jackson pleaded guilty and was sentenced in July 2008 to 300 hours

Actually, even putting aside such interferences of governments, Nakamoto considered models based on trust much more fragile than those based on proof. While asked on the P2P Foundation forum whether Bitcoin was akin to "Chaum's anonymous digital money", Nakamoto answered: "the biggest difference is the lack of a central server. That was the Achilles heel of Chaumian systems; when the central company shut down, so did the currency" (P2P Foundation, 2009-02-12). A few days later, Nakamoto wrote on the same forum: "lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them." (P2P Foundation, 2009-02-15).

3. Bitcoin: the issuing rule and the absence of a standard of money

The fact that there is no central authority in the Bitcoin system raised the problem of how bitcoins would be issued. This question, which appears highly significant for an economist, was treated incidentally in the white paper. It appeared as a by-product of another question, the incentive for nodes to support the Bitcoin network:

> By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them (Nakamoto, 2008b, p. 4).

New bitcoins are thus awarded to the node which first solves the SHA-256 cryptographic hash function associated to a block of transactions. This node is then allowed to add this "block" to the "chain". In the white paper, Nakamoto considered an additional incentive consisting in transaction fees: "If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction" (Nakamoto, 2008b, p. 4)[16]. These two mechanisms appeared to Nakamoto complementary rather than competitive. Indeed, he planned that transaction fees and the issue of new bitcoins would co-exist till the quantity of bitcoins reached a certain amount. Then, no more

of community service, a $200 fine, and three years of supervision, including six months of electronically monitored home detention. On E-gold, see Mullan, 2014, pp. 20-29.

[16] The introduction of these fees, by increasing transaction costs, may appear at odds with the Bitcoin initial project of a currency which would not "limit the minimum practical transaction size" (Nakamoto, 2008b, p. 1). Nakamoto admitted this point but still considered Bitcoin less expensive than the traditional banking system: "Bitcoin isn't currently practical for very small micropayments. Not for things like pay per search or per page view without an aggregating mechanism [...] Bitcoin is practical for smaller transactions than are practical with existing payment methods. Small enough to include what you might call the top of the micropayment range. But it doesn't claim to be practical for arbitrarily small micropayments" (Bitcointalk, 2009-2010, 2010-08-04. See also Bitcointalk, 2009-2010, 2010-06-18). The introduction of these fees appears in Nakamoto correspondence as a solution to limit "dust spam" problem. On this issue, see Bitcointalk 2020 and Bitcointalk, 2009-2010, 2010-06-18).

bitcoins would be issued and nodes would be remunerated by transaction fees only: "Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees" (Nakamoto, 2008b, p. 4).

Nakamoto announced the details of the issuing procedure in an e-mail to the Cryptography Mailing List on 8 January 2009:

> Total circulation will be 21,000,000 coins. It'll be distributed to network nodes when they make blocks, with the amount cut in half every 4 years.
> first 4 years: 10,500,000 coins
> next 4 years: 5,250,000 coins
> next 4 years: 2,625,000 coins
> next 4 years: 1,312,500 coins
> etc...
> When that runs out, the system can support transaction fees if needed. (Cryptography Mailing List, 2009-01-08. See also Bitcoin List, 2009-01-12).

The description of this process of issuing new bitcoins raises several comments.

First, it seems that a change took place in Nakamoto's view of this process, between the publication of the "white paper"-at the end of October 2008-, and the e-mail announcing the launch of Bitcoin-in early January 2009. This change concerned the amounts of the successive issues of Bitcoins over time. In the white paper, Nakamoto mentioned a "steady addition of a constant of amount of new coins" (Nakamoto, 2008b, p. 4). Again, a few days after the publication of this paper, Nakamoto wrote on the Cryptography Mailing List (2008-11-08): "coins have to get initially distributed somehow, and a constant rate seems like the best formula". Obviously, this initial view changed and the creation of new bitcoins was decided two months later at a decreasing rate.

That the "distribution schedule" of new coins had been a real question for Nakamoto is confirmed in an e-mail he sent to Hearn on 12 April 2009. The same e-mail raised another point which appears also to have been an important object of reflections on the part of Nakamoto: bitcoins being "issued in a limited, predetermined amount" (P2P Foundation, 2009-02-18) the determination of the "number of coins" needed to be settled:

> My choice for the number of coins and distribution schedule was an educated guess. It was a difficult choice, because once the network is going it's locked in and we're stuck with it. I wanted to pick something that would make prices similar to existing currencies, but without knowing the future, that's very hard. I ended up picking something in the middle. If Bitcoin remains a small niche, it'll be worth less per unit than existing currencies. If you imagine it being used for some fraction of world commerce, then there's only going to be 21 million coins for the whole world, so it would be worth much more per unit (Nakamoto, 2009-2011, 2009-04-12)

To Nakamoto, the problem of the magnitude of the pre-determined quantity of bitcoins in circulation over time was to determine *ex ante* a quantity of bitcoins which would guarantee this currency a value roughly comparable to that of existing monies such as dollar or euro. Thus, prices expressed in bitcoins would not have too many zeros nor decimals. As Nakamoto explained to Hearn one year after having launched Bitcoin, "If you're tossing around 100 000 units, it doesn't feel scarce. The brain is better able to work with numbers from 0.01 to 1000" (Nakamoto 2009-2011, 2011-01-10). The search for this "ideal" quantity of bitcoins may seem quite delusive since, as Nakamoto admitted, he had no way of knowing whether Bitcoin would be largely used or not in the future. Finally, he recognized in the same e-mail that there was a quite simple *ex post* solution to this problem: "if it gets really big, the decimal can move two places and cents become the new coins" (Nakamoto, 2009-2011, 2011-01-10).

From a monetary point of view, the pre-determined number of coins in circulation over time appears as a real singularity of Bitcoin compared to traditional currencies[17]. Nakamoto appeared fully aware of it. He was also conscious of the consequence of this singularity with respect to the relation between the quantity and the value of money. In a message he sent to a P2P Foundation forum, Nakamoto wrote: "Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes" (P2P Foundation, 2009-02-18).

In the same message, Nakamoto went even one step further. He connected this reversal of the traditional sense of causality between the quantity and the value of a currency to his will not to tie his currency to anything:

> there is nobody to act as central bank or federal reserve to adjust the money supply as the population of users grows[18]. That would have required a trusted party to determine the value, because I don't know a way for software to know the real world value of things. If there was some clever way, or if we wanted to trust someone to actively manage the money supply to peg it to something, the rules could have been programmed for that. (P2P Foundation, 2009-02-18)

This quotation highlights another element that makes bitcoin a quite singular monetary object. Indeed, currencies are usually defined with respect to a "monetary standard", that is, using Mason's definition of the term, a "criterion, or referent, of monetary policy" (1963, p. 81)[19]. Most of the time, this standard-which in the case of Mason's definition, can be assimilated to a benchmark-"purport[s] to stabilize the […] value of money in terms of some thing or things" (Mason, 1963, p. 82).

In the case of Bitcoin, the predetermined issue of coins, seems to render the selection of a monetary standard quite illusory. Since it is impossible to change the

[17] On the "Bitcoin monetary rule", see Cachanovsky 2019.

[18] It is worth noting that nowhere in his writings, Nakamoto seemed to consider the possibility of an endogenous supply of money.

[19] As stressed by Mason (1963, p. 81), the interest of this definition is that it is "free from the logical and theoretical difficulties inherent in the alternative concepts of a monetary standard. It involves no internal inconsistency, and it is consistent with abstract money and modern value theory, as well as with commodity money and classical value theory of value". On the notions of "monetary standard", see Mason, 1963; Barro and Plosser, 1983; Deleplace, 1996; Marcuzzo, Officer and Rosselli, 1997.

quantity of coins in circulation, bitcoin has no way to conform to any monetary standard. In other words, instead of first defining a monetary standard and then determining an issuing rule aiming at conforming the value of money in term of it, Nakamoto first established the issuing rule of Bitcoin and finally adopted a currency without any monetary standard.

4. The bitcoin, the Iraqi Swiss dinar and the standard of money

In a paper published in 2015, Selgin forged the concept of "Synthetic commodity money"[20], a category in which he included bitcoin. According to his definition, a synthetic commodity money has two characteristics. First, it has no nonmonetary use value *ie*, it is not a commodity. Second, it is "absolutely" rather than "contingently scarce" (Selgin, 2015, p. 93). On this second point Selgin noticed:

> the automaticity of a synthetic commodity base regime means that an economy relying upon such has no need for a monetary 'authority' at all, meaning one charged with either discretionary management of the monetary base or the enforcement of a monetary rule […] supply is determined once and for all by artificially arranged resource constraints (pp. 94-5).

Historical examples of such "synthetic commodity monies" appear quite scarce. In addition to Bitcoin, Selgin (2015, pp. 95-6) noticed the Iraqi Swiss dinar[21].

The Iraqi Dinar entered circulation in 1932 as the official money of Iraq. It was first issued by a currency board, and from 1949 by the newly created National Bank of Iraq (which became the Central Bank of Iraq in 1956). The Iraqi dinar was pegged at par with the Pound Sterling until 1959. Then, without changing its value, the peg was switched to the US dollar at the rate of ID 1 = US$2.80 (Metz, 1990, p. 281). This ratio underwent several changes in the 70's. In 1982, the Iraqi dinar was devaluated 5 per cent to an official value of 1 dinar = US$ 3.2169. This official value remained until 1990 and the Gulf War. At the end of the war, in 1991, the Iraqi dinar had felt to 1/600 of its official value (Kitamura, 2022, p. 33). The United Nations sanctions prevented the Iraqi Government from importing these notes which were printed abroad by the British private company "De la Rue". Thus, the Iraqi Government started issuing new bank notes known as "Saddam" dinars, in opposition to the old dinars which had been printed using Swiss-engraved plates. These were thus named "Swiss" dinars. The "Saddam" dinars were used by the Sunnis and Shiite's of southern Iraq. In the north of Iraq, which was a *de facto* Kurdish protectorate, people had no opportunity to exchange their old dinars for new ones.

[20] This notion was then adopted, among others, by Baur, Hong and Lee, 2018, p. 178; Nabilou, 2020, p. 42; Cachanovsky, 2022, p. 15; Mann, Taheri and McWhirter, 2022, p. 203. See also Desmedt and Lakomski-Laguerre, 2020, pp. 150-1.

[21] On the Iraqi Swiss dinar, see Metz, 1990, p. 281; King, 2004, pp. 7-10; Kitamura, 2022, pp. 30-33. Selgin (2015, p. 96, n. 12) also mentioned the Somali shilling (which will not be considered in the present paper) as a synthetic commodity money. On the Somali shilling, see Mubarak, 2002; Luther, 2015; Luther and White, 2016.

Then, the Swiss dinars continued to be used in the North even though they were not legal tender nor backed by any institution anymore. King (2004, p. 8) summed up the situation as follow: "no Swiss dinar notes were issued after 1989, and since there was no issuing authority there was at most a fixed, and probably a declining money stock in the North".

After the end of the fall, in 1991, the Swiss Dinar recovered part of its value. It stabilised between July 1998 and July 2002 at a rate between 17 and 19 Iraqi Swiss dinars for US$1 (King, 2004, p. 8). Then, as the prospect of an end to the Saddam regime increased, the Swiss dinar raised to reach in May 2003 the rate of 1 USD for 6 dinars (King, 2004, p. 8). The Iraqi Swiss dinar disappeared in early 2004 when a new dinar was printed and exchanged for both "Saddam" and "Swiss" dinars. This exchange was made at the rate of 1 Swiss dinar = 150 Saddam dinar. According to King, who first drew attention to the Iraqi Swiss dinar, this experience illustrated "the importance of expectations about the *future* of monetary institutions" (2004, p. 7)[22]. To Selgin, who adopted a quite different point of view, this Iraqi Swiss dinar demonstrated the "viability of a synthetic commodity currency" (2015, p. 96)[23].

The point made by Selgin is that both the bitcoin and the Swiss dinar belong to what he defined as the category of synthetic commodity money. This point seems to be enforced by Mason's conception of the monetary standard. Indeed, according to him, "if monetary decisions are made without any ascertainable criterion for the choices among alternatives [of monetary policy], then there is no monetary standard" (Mason 1963, p. 81). Thus, because it allowed no monetary policy, the bitcoin, just like the Swiss dinar, has no monetary standard.

Mason's conception of the monetary standard may however appear somewhat restrictive. In particular, it excludes the use of the standard as a measure of the value of money. Indeed, considered as such, the standard pertains, even if an inexistent or inappropriate monetary policy prevent the value of money to conform to it. Moreover, it may even be said that this function of the standard takes its full meaning precisely when the value of money departs from it.

This conception of the monetary standard as a measure of the value of money is not included by Mason in what he called a "monetary standard". However, it does not seem to contradict his genuine conception of the standard as a "criterion" or a "referent" of monetary policy, but rather to enhance it. Moreover, this conception of the monetary standard appears to be shared by economists of different theoretical sensibilities. David Ricardo for example considered as "a truth" the fact that in 1811 "gold [was] no longer in practice the standard by which our currency is regulated" (Ricardo, 1951-73, vol. 3, p. 255). At this time, the price of the standard (gold) deviated from the official definition of the pound sterling of nearly 20% (Ricardo, 1951-73, vol. 3, p. 132). However, this did not prevent him from comparing the currency to the "lost" standard, since "it can only be by a comparison to this standard that its regularity, or its depreciation, may be estimated" (Ricardo, 1951-73, vol. 3,

[22] See also Kitamura, 2022, p. 31.

[23] For a critical view of Selgin's position, see Senner and Sornette, 2019, p. 975.

p. 65). The same use of the standard as a measure of the value of money was also advocated by Keynes in *A Treatise on Money*. The "standard" was not the same than at the age of Ricardo, but its use pertained: "the index number of the price of the composite commodity representative of consumption is the standard by which units of purchasing power are measured" (Keynes, 1930, p. 49)[24].

Finally, this use of the standard as a measure of the value of money appears clearly at works in contemporary analysis of the Iraqi Swiss dinar. This is for example the comparison of the current value of the swiss dinar to its legal definition in dollars which led Kitamura (2022, p. 33) to assert that in 1991, the Iraqi dinar had felt to 1/600 of its official value. Again, this is an examination of the price of the standard-the exchange rate with US dollar-in the mid 1990's, that led Selgin to conclude that contrary to the Saddam dinars, the Swiss dinars "held their value" (Selgin, 2015, p. 96). Thus, even when the monetary standard is no longer effective in practice, its function as a measure of value of the monetary unit remains.

Now, as explained at the end of the last section, in the case of Bitcoin, there is no standard *at all*. The pre-determined quantity of bitcoins in circulation over time prevents their value from conforming to any standard. It then appears both unnecessary and illusory to establish such a standard. This of course, makes sense. However, it also deprives Bitcoin of a monetary standard considered as a criterion for ascertaining and measuring changes in the value of bitcoins. Such variations are then impossible to determine. Using Ricardo's words: "if we adopted a currency without a standard […] the depreciation [or appreciation] could not admit of proof, as it might always be affirmed that commodities had risen [or fallen] in value, and that money had not fallen [or risen]" (Ricardo, 1951-73, vol. 4, p. 62).

5. Conclusion

The fact that the value of bitcoin was never defined with respect to something external to it-a standard-makes bitcoin a quite singular monetary object. Indeed, this distinguishes bitcoin, even from other types of Synthetic commodity monies such as the Iraqi Swiss dinar. This particularity of Bitcoin has not been stressed by the economic literature on the subject. However, the absence of a standard, and then of a criterion by which the variations in the value of bitcoin can be estimated, seemed to have been determinant in the subsequent development of cryptocurrencies. It can be seen, for example, as what precipitated the emergence of the following generation of cryptocurrencies, which values were connected-in one way or another-to a commodity, a currency or a basket of goods or of currencies. This second generation of cryptocurrencies, generally called stablecoins, brought the role of the monetary standard back to the forefront. However, most of the time, this was done at the expense of what Nakamoto introduced as the "spirit" of the genuine Bitcoin project.

[24] On the extensive use of the notion of money as purchasing power made by Keynes, see Graziani, 1996.

Bibliography

Ammous, S. 2018. Can Cryptocurrencies Fulfil the Functions of Money? *The Quarterly Review of Economics and Finance*, vol. 70, pp. 38-51

Barro, R. B. and Plosser, C. I. (eds) 1983. Conference on Alternative Monetary Standards, *Journal of Monetary Economics*, vol. 12, no. 1

Baur, D. G., Dimpfl, T. and Kuck, K. 2018. Bitcoin, Gold and the US Dollar-A Replication and Extension, *Finance Research Letters*, vol. 25, pp. 103–110

Baur, D. G.; Hong, K. and Lee, A. D. 2018. Bitcoin: Medium of Exchange or Speculative Assets? *Journal of International Financial Markets, Institutions and Money*, vol. 54, pp. 177-189

Bitcoin List, 2008-2010. Bitcoin List Emails, Bitcoin List Email Series Authored by Satoshi Nakamoto | Satoshi's Archive [date last accessed: 4 February 2023]

Bitcointalk, 2010. Flood Attack 0.00000001 BC, Flood attack 0.00000001 BC (bitcointalk.org) [date last accessed: 4 February 2023]

Bitcointalk, 2009-2010. Bitcointalk Posts, Forum Posts | Satoshi Nakamoto Institute [date last accessed: 4 February 2023]

Bjerg, O. 2016. How is Bitcoin Money? *Theory, Culture & Society*, vol. 33, no. 1, pp. 53-72

Böhme, R., Christin, N., Edelman, B. G. and Moore, T. 2015. Bitcoin: Economics, Technology, and Governance, *Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213-238

Bouoiyour, J. and Selmi, R. 2015. What Does Bitcoin Look Like? *Annals of Economics and Finance*, vol. 16, no. 2, pp. 449–492

Bouri, E., Kristoufek, L., Lucey, B., Roubaud, D. and Shahzad, S J. H. 2019. Is Bitcoin a Better Safe-Haven Investment than Gold and Commodities? *International Review of Financial Analysis*, vol. 63, pp. 322–30

Brunton, F. 2019. Digital Cash. *The Unknown History of the Anarchists, Utopians, and Technologists who created Cryptocurrency*, Princeton and Oxford, Princeton University Press

Cachanosky, N. 2022. Can Cryptocurrencies Become a Commonly Accepted Means of Exchange? in J. L. Caton (ed.) 2022, pp. 13-28

Cachanosky, N. 2019. Can Bitcoin Become Money? The Monetary Rule Problem, *Australian Economic Papers*, vol. 58, no. 4, pp. 365-74

Caton, J. L. (ed.) 2022. *The Economics of Blockchain and Cryptocurrency. A Transaction Costs Revolution*, Cheltenham (UK) and Northampton (US), Edward Edgar

Cointelegraph, 2014. Satoshi Nakamoto's Email Account Hacked, Satoshi Nakamoto's Email Account Hacked (cointelegraph.com) [date last accessed: 4 February 2023]

Corbet, S., Larkin, C., Lucey, B., Meegan, A. and Yarovaya, L. 2018. Exploring the Dynamic Relationships Between Cryptocurrencies and Other Financial Assets, *Economics Letters*, vol. 165, pp. 28–34

Cryptography Mailing List, 2008-2009, Cryptography Mailing List Email, Cryptography Mailing List Email Series Authored by Satoshi Nakamoto | Satoshi's Archive (bitcoin.com) [date last accessed: 4 February 2023]

Dai, W. 1998. B-Money, an Anonymous, Distributed Electronic Cash System, http://www.weidai.com/bmoney.txt [date last accessed: 4 February 2023]

Deleplace, G. 1996. Does Circulation need a Monetary Standard? in G. Deleplace and E. J. Nell (eds) 1996, pp. 305-29

Deleplace, G. and Nell, E. J. (eds) 1996. *Money in Motion. The Post Keynesian and Circulation Approaches*, London, Macmillan

Desmedt, L. and Lakomski-Laguerre, O. 2021. Les monnaies cryptographiques : vers une révolution de la confiance ? *Revue française d'histoire économique*, no. 16, pp. 98-112

Desmedt, L. and Lakomski-Laguerre, O. 2020. Du monnayage au crypto-monnayage, *Dialogues d'histoire ancienne*, additional issue no. 20, pp. 143-56

Desmedt, L. and Lakomski-Laguerre, O. 2015. L'alternative monétaire Bitcoin : une perspective institutionnaliste, *Revue de la Régulation*, no. 18

Dodd, N. 2017. The social life of Bitcoin, *Theory, Culture & Society* , vol. 35, pp. 35-56

Dodd, N. 2014. *The social life of Money*, Princeton, Princeton University Press

Dwyer, G. P. 2015. The Economics of Bitcoin and Similar Private Digital Currencies, *Journal of Financial Stability*, vol. 17, pp. 81-91

Dyhrberg, A. H. 2016a. Bitcoin, Gold and the Dollar - A GARCH Volatility Analysis, *Finance Research Letters*, vol. 16, pp. 85–92

Dyhrberg, A. H. 2016b. Hedging Capabilities of Bitcoin. Is It the Virtual Gold? *Finance Research Letters*, vol. 16, pp. 139-44

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

Goutte, S., Guesmi, K. and Saadi, S. (eds) 2022. *Cryptofinance A New Currency for a New Economy*, Hackensack (US) and London (UK), World Scientific Publishing

Graziani, A. 1996. Money as Purchasing Power and Money as a Stock of Wealth in Keynesian Economic, in G. Deleplace and E. J. Nell (eds) 1996, pp. 139-54

Hazlett, P. and Luther, W. J. 2020. Is Bitcoin Money? And What that Means. *The Quarterly Review of Economics and Finance*, vol. 77, pp. 144-149

Hearn, M. 2016. The Resolution of the Bitcoin Experiment. https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7 [date last accessed: 4 February 2023]

Keynes, J. M. 1930. *A Treatise on Money: The Pure Theory of Money*, in D. Moggridge (ed.) *The Collected Writings of John Maynard Keynes*, London, Macmillan, vol. V, 1973.

King, M. 2004. The Institutions of Monetary Policy, *American Economic Review*, vol. 94, no. 2, pp. 1–13

Kitamura, Y. 2022. *Quest for Good Money. Past, Present and Future*, Singapore, Springer

Klein, T., Thu, H. P. and Walther, T. 2018. Bitcoin Is not the New Gold-a Comparison of Volatility, Correlation, and Portfolio Performance, *International Review of Financial Analysis*, vol. 59, pp. 105-116

Lee Kuo Chuen, D. (ed.) 2015. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instructments, and Big Data*, Waltham, Elsevier

Luther, W. J. 2019. Getting off the Ground: The Case of Bitcoin, *Journal of Institutional Economics*, vol. 15, no. 2, pp. 189-205

Luther, W. J. 2015. The Monetary Mechanism of Stateless Somalia, *Public Choice*, vol. 165, no. 1-2, pp. 45-58

Luther, W. J. and White, L. H. 2016. Positively Valued Fiat Money after the Sovereign Disappears: The Case of Somalia, *Review of Behavioral Economics,* vol. 3, no. 3-4, pp. 311-34

Mann, J., Taheri, S. and McWhirter, A. 2022. The Nexus between Cryptocurrencies, Currencies and Commodities: A Primer, in S. Goutte, K. Guesmi and S. Saadi (eds) 2022, pp. 191-206

Marcuzzo, M. C., Officer, L. H. and Rosselli, A. 1997. *Monetary Standards and Exchange Rates*, London, Routledge

Mason, W. E. 1963. *Clarification of the Monetary Standard*, University Park, Pennsylvania State University Press

Maurer, B., Nelms, T. C. and Swartz, L. 2013. "When perhaps the real problem is money itself!": the practical materiality of Bitcoin, *Social Semiotics*, vol. 23, no. 2, pp. 261-277

Maurer, B., Nelms, T. C., Swartz, L. and Mainwaring, S. 2018. Social Payments: Innovation, Trust, Bitcoin, and the Sharing Economy, *Theory, Culture & Society*, vol. 35, no. 3, pp. 13–33

Metz, H. C. (ed.) 1990. *Iraq: A Country Study*, Washington, Federal Research Division

Mubarak, J. A. 2002. A Case of Private Supply of Money in Stateless Somalia, *Journal of African Economies*, vol. 11, no. 3, pp. 309-325

Mullan, P. C. 2014. *The Digital Currency Challenge: Shaping Online Payment Systems through US Financial Regulations*, New York, Palgrave Macmillan

Nabilou, H. 2020. The Dark Side of Licensing Cryptocurrency Exchanges As Payment Institutions, *Law and Financial Markets Review*, vol. 14, no. 1, pp. 39-47

Nakamoto, S. 2009-2011. Emails to Mike Hearn, Email Exchange Between Satoshi Nakamoto and Mike Hearn | Satoshi's Archive (bitcoin.com) [date last accessed: 4 February 2023]

Nakamoto, S. 2009. Emails to Dustin Trammel, Satoshi Nakamoto and Dustin Tremmel exchange emails on Bitcoin first release | Satoshi's Archive [date last accessed: 4 February 2023]

Nakamoto, S. 2008b. Bitcoin: A Peer-to-Peer Electronic Cash System, http://www.bitcoin.org/bitcoin.pdf

Nakamoto, S. 2008a. Electronic Cash without a trusted Third Party, https://nakamotostudies.org/literature/ecash.html [date last accessed: 4 February 2023]

Orléan, A. 2019. La communauté bitcoin, *Esprit*, no. 436, pp. 47-58

P2P Foundation, 2009-2014. P2P Foundation Forum Posts, Bitcoin open source implementation of P2P currency - P2P Foundation (ning.com) [date last accessed: 4 February 2023]

Ricardo, D. 1951–1973. *The Works and Correspondence of David Ricardo*, 11 vols. Edited by P. Sraffa, with the collaboration of M.H. Dobb, Cambridge, Cambridge University Press

Selgin, G. 2015. Synthetic Commodity Money, *Journal of Financial Stability*, vol. 17, special issue, pp. 92-9

Senner, R. and Sornette, D. 2019. The Holy Grail of Crypto Currencies: Ready to Replace Fiat Money? *Journal of Economic Issues*, vol. 53, n°. 4, pp. 966-1000

Smales, L. 2019. Bitcoin As a Safe Haven: Is It even Worth Considering? *Finance Research Letters*, vol. 30, pp. 385–393

Söderberg, G. 2018. Are Bitcoin and Other Crypto-Assets Money? *Economic Commentaries*, vol. 5, pp. 1-14

Weber, B. 2016. Bitcoin and the Legitimacy Crisis of Money, *Cambridge Journal of Economics*, vol. 40, no. 1, pp. 17-41

Yermack, D. 2015. Is Bitcoin a Real Currency? An Economic Appraisal, in Lee Kuo Chuen 2015, pp. 31-44