On Cryptocurrencies

Eduardo Salazar*

Forctis AG
Samstagernstrasse 55
CH-8832 Wollerau
Switzerland

18th April 2018

Abstract. This paper presents an overview of virtual currencies, placing a particular focus on the so-called cryptocurrencies: actors, their underlying motivations, its emergence, recent developments and prevailing trends; done against the backdrop of economic theory, history, sociology and economic anthropology as they have been repeatedly (and competitively) applied to explain the genesis and logic of money.

The aim is to properly characterise cryptocurrencies and to try answer, through the analysis of that body of work and other evidence, two simple questions. Firstly, what are they? Secondly, and perhaps even more importantly, what could they become?

It constitutes `Part #1` of our `White Paper` and is meant to "set the scene" for a more ambitious programme in `Part #2`. There, we will outline an alternative approach and a proposal for the implementation of a cryptocurrency with "desirable" properties. In other words, it will attempt to deliver a substantiated answer to yet another simple question: how?

Keywords: `Money; History; Coordination; Cryptocurrency`

JEL codes: `B10, B21, C78, E42`

1. Introduction

The central role that money plays in modern society can hardly be disputed. It is indeed one of the oldest human creations and has been repeatedly used as a proxy laboratory for testing new ideas. Money has therefore been subject, throughout history, to sudden and profound changes prompted by fiscal policy failures, in the wake of armed conflicts or even induced by famines. Societies have assimilated the transformations of money in multiple ways, sometimes viewing them as the (perhaps inevitable) by-product of the evolution in social order. Those changes, at times, have ended in success, but there have also been a good share of failures, and unsurprisingly not less painful regressions.

* The author thanks Hugo Scolnik, Nicolas Jacquemart, Jake Sroczynski and Julia Panova for helpful comments and suggestions.

To some degree, every monetary experiment in history reflects a practical attempt at answering a rather simple question: "what is money?"[I] It frequently leads to a second (and not less important, nor completely separate) question: "what should money be made of?"[II]

Questions that emerge from time to time, despite the fact there are few things in life as deeply embedded or determined as money. It has also been argued that "understanding money is a matter of understanding ourselves"[1] yet people routinely make no effort (conscious or otherwise) to ponder the intrinsic qualities of money, nor think about its "meaning" on those everyday occasions when money is "put into use."[2] Indeed a remarkable feat, because money deeply penetrates every social structure and regulates, at times in a very explicit way, the relationships between people.

In recent times, however, a particular set of conditions have propelled discussions about money to centre stage.

Two coinciding processes have brought money back into everyday conversation. On the one hand, we're seeing technological innovations that are transforming social interactions in ways not seen before,[3] considering both the speed of change and the number of touchpoints being continuously added. On the other hand, this technological push is taking place as people are managing their way out of the 2007-2008 global financial crisis. In principle seemingly unrelated events, yet, once taken jointly, they help explain the mechanics leading social actors to reopen the debate about the very notion of money.

[1] See Rowe (1997).

[2] Say, when going to buy groceries, shopping for a flight on the Internet or paying for a book.

[3] Consider that by late 2007, just a year after publicly opening the platform to anyone over 13 years old, Facebook had roughly 55 million monthly active users (the number of unique users logging to or enaging in an action on the platform during the previous 30 days as of the date of measurement). To put in perspective, that same statistic at the end of 2017 was about 2 billion. Twitter had nearly half a million monthly active users by mid-2007, compared to roughly 330 million at the end of 2017. In fact, it is estimated that just over 3 billion people (or 40% of the world's population) is nowadays active on some type of social media platform. The "usability revolution" was brought by the iPhone, launched by Apple in June 2007 (with Android smartphones appeared a year later). By late 2017 there were about 5 billion smartphone users worldwide, a 68% penetration. See https://bit.ly/2BDdVTz for more details.

Such conversations have drawn on cultural repertoires, political ideologies, particular ways of understanding the undercurrents of social processes[4] and an idiosyncratic knowledge about how the economy works that are frequently translated into justifications as to how it "ought to" work. That debate is hardwired in the "search" by individuals and communities for tools, possibly imperfect or incomplete but tools nevertheless, to help them navigate the uncharted landscape brought by the financial crisis.

The influence of social media, and in more general terms modern online communications,[5] should not be understated. It has even provided an unprecedented access to "the inner workings of private worlds"[6] making them an active ingredient of this search process.

Along the road, an ingeniously designed innovation made its way towards centre stage. Its name? Bitcoin.[7]

Somebody (or a group of people, it's still unclear to this date) under the pseudonym Satoshi Nakamoto posted in 2008 a paper to a cryptography mailing-list proposing a new electronic cash protocol.[III]

Bitcoin included a couple of innovative features[IV] and became an object of interest primarily amongst technology geeks fascinated by Tim May's crypto-anarchy manifesto.[V] It took time to mobilise people beyond those groups of crypto-enthusiasts, mostly libertarians,[8] but nowadays Bitcoin has acquired such an appeal some commentators equate it to the level of a religion. Bitcoin has also opened new streams of research into applications of the blockchain, and more generally, into the adoption of the distributed ledger technology[9] it helped to popularise.[VI]

[4] Interestingly enough, mostly dictated by the dynamics of local interactions rather than a regional or even a world-view.

[5] The multiple "screens" used nowadays for interaction throughout our daily journeys, platforms and even the "identities" people assume online.

[6] See Venturini and Latour (2009).

[7] In broad terms, the nomenclature proposed by He *et al.* (2016) will be adopted throughout. It separates "digital" from "virtual" currencies by considering the latter to be any currency not denominated in legal tender and not issued by central banks. Bitcoin is therefore a specific class of virtual currency.

[8] Wei Dai began his presentation of b-money by acknowledging he was "fascinated by Tim May's crypto-anarchy."

[9] There are differences between the standard blockchain protocol and distributed ledger technology, or DLT. The former refers to platforms specifically designed to be censorship resistant, achieved through extreme decentralisation coupled to economic incentives; in turn, DLTs are permissioned architectures that could use (or not) the blockchain as approach, but decentralisation involves a number of known, pre-approved participants.

Be that as it may, it pays to look at Nakamoto's motivations. Comparing the interactions through different outlets (e.g. mailing lists, forums, records of e-mail exchanges) that took place between 2008 and early 2009, the best summary can be found in a short yet revealing discussion in the P2P foundation forum, and particularly Nakamoto's Bitcoin announcement on February 11, 2009.[10]

> 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 ... [until] strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what. It's time we had the same thing for money.

Satoshi sets Bitcoin objective(s) quite clearly. He subsequently wrote that

> [a] 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. I think this is the first time we're trying a decentralized, non-trust-based system.[VII]

Some members of the P2P community expressed a positive reaction, but others raised objections mostly focusing around the potential impact of Bitcoin's design on the token price stability.[VIII] In the subsequent debate Nakamoto admitted "there is nobody [in Bitcoin] to act as Central Bank or Federal Reserve to adjust the money supply" adding it would have required "a trusted [third] party to determine the value, because I don't know a way for software to know the real world value of things."[11]

[10] See http://bit.ly/2tBX7h7.
[11] Underlined mine.

Nakamoto hence argued this new coin was

> more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes. As the number of users grows, the value per coin increases. It has the potential for a positive feedback loop; as users increase, the value goes up, which could attract more users to take advantage of the increasing value.[12]

Judging by the exchanges taking place in the SourceForge forum and elsewhere Nakamoto used to promote Bitcoin, the platform was not enjoying much traction during the early months of 2009. The term "cryptocurrency" that came to encompass bitcoin[13] emerged during this period as a strategy to help promote the concept. That effort included a revamp of the `bitcoin.org` site steering the focus away from the code and towards ideology,[IX] particularly the role that anti-capitalists and anarcho-capitalists[14] alike assigned to "institutions"[X] (e.g. political cadres, central banks) and the "banking elites" as being responsible for the financial meltdown just a year before.[XI] The 2007-2008 global crisis is famously known to have been a source of inspiration to Satoshi, but it was not before those changes that ideology was brought so prominently to the fore.[15]

The creation of bitcoin, the P2P cryptocurrency that (after many failed past attempts) managed to capture people's imagination, can therefore be seen as a blend of determination, opportunism and some contradictions. More importantly, it reflects a practical translation of ideology into a monetary experiment from the grassroots, at scale, seeping into the mood of an increasing number of people.

[12] February 18, 2009.

[13] In the absence of a specific name, lowercase **b** gradually became the convention adopted to denote the token, leaving uppercase **B** to denote the Bitcoin protocol.

Over time, the word "cryptocurrency" permeated to other "coins" later developed either as forks or simply taking inspiration from Bitcoin. The word has recently been officially added in March 2018 to Merriam-Webster's English dictionary, having found its way to Oxford Dictionaries in May 2014 (only in its online edition, known as ODO, that focuses on modern meanings and uses of words) and following the addition of the word "Bitcoin" in August 2013.

[14] Or right-libertarians, as some call them.

[15] The Bitcoin "genesis block" famously contains the headline that appeared in The Times on January 3, 2009, as "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

Take for example Bryce Wilcox, or *Zooko* as he is best known.[16] In a blog post on January 9, 2009, he openly expressed his support for a currency like bitcoin

> [which] everyone can cheaply and conveniently use but which no-one has the power to manipulate. No-one has the power to inflate or deflate the currency supply, no-one has the power to monitor, tax, or prevent transactions. Truly the digital equivalent of gold, during the times and places when gold was the universal currency.[XII]

In summary, it could be argued the tendency to use gold as reference stems from pre-conceptions of value based on the current relative worth of both metals, rather than adherence to historical accuracy.

Despite the ideologically loud (and to no surprise, radical) voices on the Internet and elsewhere, the question that has yet to be properly and rigorously answered is if, and how, cryptocurrencies could "work." But, first, it will prove useful to review some concepts and their background.

2. Currency and Money

Here the word, there the meaning.
The money, and the cow that you can buy with it.
`Wittgenstein, 1958, p. 49`

It is fair to say that the words *currency* and *money* are nowadays used interchangeably in everyday speak, almost without any thought.

Some clarifications, however, might be necessary. For a start, the word *currency* has its origins in *currentia*, a Medieval Latin word derived from the Latin *curro* meaning to run, to move quickly or to flow. Cicero used it to imply general acceptance or recognition. In a

[16] Wilcox is one of the core developers of Tahoe-LAFS, a free and open decentralized cloud storage system. See http://bit.ly/2FA1Ipp. He created a blog that Nakamoto had linked to `bitcoin.org` (alongside pointers to Wei Dai's b-money and Nick Szabo's bit-gold sites in a "Related Links" section) during the early days of Bitcoin's site. It dissapeared completely from sight at the time `bitcoin.org` changed its look and messaging by late 2009. In 2016 he developed the privacy coin ZCash.

compilation of his speeches under the title "On the Agrarian Law"[17] it can be read

> *cur non eosdem cursus hoc tempore quos L. Cotta L. Torquato consulibus cucurrerunt?*[18]

The phrase can be translated as "why not follow the same course[19] as that taken at the time of the consulship of L. Cotta and L. Torquato?" In the context of Cicero's phrase to "follow the same course" means "to accept" hence, from an etymological standpoint, becoming "a" currency embodies the ability to circulate due to its general acceptance.[20]

Concerning the origin of the word *money*, throughout history there has been some controversy but the prevailing consensus is to trace it back to the Latin word *Moneta* or "who warns," derived from *monere*, the Latin for warning.[21] Many historians make the connection to an episode that took place about 300 BC when the Roman mint was relocated to the temple dedicated to Juno Moneta.[XIII]

It is therefore assumed the word *Moneta* gradually became associated with "mint" and later, with the word money.[22] Centuries later, the "flow" property of currencies permeated to the concept of money (or more generally, a means of payment) in Hobbes' *Leviathan*, who defines it as

> the means [that] measures all commodities, movable and immovable... passeth from man to man within the Commonwealth, and goes round about, nourishing, as it passeth, every part thereof. [23]

[17] M. Tullius Cicero (1856), 2.17.44. It consists of four speeches where Cicero condemned the agrarian reforms (seeking to redistribute land for farming to the landless poor in Rome) proposed by Publius Servilius Rullus in 63 BC.

[18] The names correspond to Lucius Aurelius Cotta and Lucius Manlius Torquatus, both elected Roman consuls in 65 BC.

[19] Or *eosdem cursus currere*.

[20] Logically, if something is repudiated it would not find it easy to change hands.

[21] Some authors emphasise the link to $\mu\nu\eta\mu o\sigma\upsilon\nu\eta$ or *mnemosyne*, the Greek goddess of memory and remembrance. By implication, money is understood as a materialisation of memory. See, e.g. the paper by Miano (2012).

[22] Cicero, in his *Letters to Atticus* (1913, 8.7.3) wrote *ad Philotimum scripsi de viatico sive a Moneta –nemo enim solvit– sive ab Oppiis tuis contubernalibus* which can be translated as "I wrote to Philotimus about providing me with money for the journey either from the Mint, for no-one is paid now, or from your banking friends."

[23] In Hobbes (1651, 24.11). This same train of thought was reflected, e.g. in a pamphlet by A. Hamilton compiled as part of *The Federalist* where he wrote "[m]oney is, with propriety, considered as the vital principle of the body politic; as that which sustains its life and motion, and enables it to perform its most essential functions." (see N^{o} 30, 1787). But others strongly disagreed. H. Dunning Mcleod, in his *Theory and Practice of Banking* wrote

> [w]e must observe that the word *Circulation* is often used in a very corrupt sense... more especially by American writers, for whence we believe the absurdity of calling money currency originated... [w]e shall always use the words currency and circulation to mean different things... [that] do not bear any fixed relation to each other. See Mcleod (1866, p. 26; underlined mine).

Such connection is reflected in how modern economics define currency, e.g. as "money currently circulating in a country and available for immediate use as a medium of exchange"[24] or as "that component of a country's money stock that literally circulates from hand to hand."[25]

Despite current convention, if anything, the above discussion seems to suggest that the notions of currency and money ought to be differentiated. However, this is a separate debate (although at times wrongly intertwined) from that concerning the origin of money, something we tackle next.

3. On the origin of money

Only understand the origins of an institution or instrument and you will find its present-day role much easier to grasp.
N. Ferguson, 2008, p. 12

In order to explain the origin of money, it is necessary to trace the conditions, historical or otherwise, that led to its emergence. Despite the heading for this section resembling that of Book I, Chapter IV in Adam Smith's *Wealth of Nations*[26] the approach pursued here is certainly not confined to presenting an "invisible hand" account of the evolution of money.[27]

It provides, however, a good starting point,[28] for it permeated into the neoclassical explanation[29] of money's origin presented by

[24] Rutherford (2002).
[25] Pearce (1992).
[26] See A. Smith (1859 [1776]).
[27] Adam Smith became a towering figure of the Scottish Enlightement, including the likes of Hume, Ferguson and Mandeville. In his *magnus opus*, Smith's chapter had as title "Of the Origin and Use of Money." As for Smith's much revered concept of "invisible hand," perhaps a curious fact is that the term only appears three times in his book.

It also closely resembles the title of Menger's paper by the title "On the Origins of Money."
[28] Smith considered human beings as having a distinctive "propensity to truck, barter, and exchange one thing for another" (op.cit., book I, ch. II, p. 6) despite arguing that barter is problematic because commodities are heterogeneous, sometimes perishable, and most likely imperfectly divisible (op.cit, book I, ch. V). It made sense, therefore, to have "a common stock" so that "every man may purchase whatever part of the produce of other men's talents he has occasion for" (op.cit., book I, ch. II, p. 8). That said, Smith does not go beyond making a statement, as he nowhere discusses how a commodity enjoying "general acceptance" comes into existence.
[29] See also note XVII, par. 1, for completeness.

W. Stanley Jevons[30] and Carl Menger.[31] To Menger, money emerged as the unintended consequence of everyday, dispersed actions by economic agents, prescindient of any form of "common interest" driving them. Going back to primitive societies,[32] Menger saw barter as the precursor of money.[33] He wrote that

> [m]en have been led, with increasing knowledge of their individual interests, each by his own economic interests... even without any regard to the common interest, to exchange goods destined for exchange –their "wares"– for other goods equally destined for exchange[34]

taking place

> as the spontaneous outcome, the unpremeditated resultant, of particular, individual efforts of the members of a society[35]

adding that

> [by] the devious way of a mediate exchange,[36] he gains the prospect of accomplishing his purpose more surely and economically than if he had confined himself to direct exchange.[37]

The above logic, however, can be disputed. To be considered as a medium of exchange, any commodity (be it rice, salt, cowries or gold) has to be quickly verifiable, at a low enough cost by anyone entering into a transaction (otherwise, it makes no economic sense) so that each party can be assured the same value is given up as is received. If its

[30] See Jevons (1919 [1875]).

[31] See Menger (1981 [1871], 1892). The work by Jevons and Menger shows great similarities in terms of how they rationalised individual's behaviour and the operation of markets (see Peart, 1998) but, of the two, it was Menger who proposed a more advanced theory of money.

[32] By that implying a community of people not governed by a State.

[33] As Marshall wrote in his *Principles* it follows the precept that *natura non facit saltum* or "nature does not take leaps" in the economic world (1890 [2013], book IV, ch. 9, p. 207). Going along Menger's train of thought, the implication is that money's value today is a reflection of the non-monetary use value of some commodity in the past, just before it became adopted as medium of exchange.

[34] See Menger (op.cit, p. 248).

[35] Ibid., p. 250. Note, in passing, that reaching equilibrium in a barter economy requires a reasonably even distribution of endowments and needs across society, and that all goods are treated symmetrically.

[36] That is, money. Upon discussing Menger's microeconomic foundations of money, Endres (1997, p. 172) wrote "[t]he use of money [in Menger] cannot be precisely scheduled; it acts as a stock against the disappointment of individuals' plans in uncertain conditions."

[37] Ibid., p. 248.

value becomes recognized and agreed upon, it can then be adopted as unit of account. Contracts, be it for immediate or future delivery[38] can be easily expressed if a unit of account is available to the intervening parties. This combination of factors leads to the general acceptance of such commodity as a medium of exchange; in other words, the stage when it becomes the commodity, amongst the economic goods available to society, having the highest subjective probability of trade.

Menger's approach sees a more formal treatment in Jevons' edifice, built on the existence of the problem of wants in barter.[39] Money is also treated by Leon Walras, taking a different angle to Menger's. In Walras, money derives its value from the difficulties of the exchange process (seemingly confined to bilateral trades only) and not from the direct utility it could provide. In other words, money provides a service.[XV]

Finding a trading partner in a barter environment might be costly, both in effort and time; something that both Menger and Walras acknowledged. Consequently, by adopting the commodity having the lowest transaction cost from the basket of goods available,[40] then it would be possible for a society to achieve allocations that could not be otherwise achievable.[XVI]

Given the existence of transaction costs whenever there is an absence of a double coincidence of wants, there is a role for money.

[38] That is, the possibility to engage in inter-temporal trade.

[39] Jevons (op.cit., ch. 1) assumed there are three categories of "wants," as follows.

- `Wants of Coincidence in Barter`: finding "two persons whose disposable possessions mutually suit each other's wants";
- `Wants of a Measure of Value`: determining "at what rate is any exchange to be made"; and
- `Wants of Means of Subdivision`: the problem of suitably dividing "many kinds of goods."

Much of the literature limits to the coincidence of wants problem, basically, that under pure barter[XIV] not only one must want what the other party has on offer, but the other party has also to want what one is offering in exchange.

[40] The logic is simple. If the cost of converting a given commodity into "something else" is the lowest amongst all of the other commodities available in an economy (or as Starr [2012] likes to say, the commodity with the lowest bid to ask spread) then it becomes, de facto, the most liquid asset. That asset is money. In his work on post-war cigarrette money, Bignon commented "the liquidity of money comes from its sole role of medium of exchanges"(2006, p. 2). In other words, the fact that cigarrettes were accepted as money meant they carried a positive exchange value, hence people were willing to hold them.

So, framing the origin of money in terms of a commodity used as a "carrier of value between successive transactions"[41] using barter as precursor[42] became the cornerstone of a school of thought and narrative known as the Commodity or Metallist[43] approach to money,[XVII] also referred to as the Austrian School.[XVIII]

Early on, however, other scholars took a completely opposite stance, arguing the question of "intrinsic value" (emerging from the association to physical commodities in barter) is immaterial as precondition for characterising money. To them, the key aspect separating money from other goods is simply its unique ability to cancel debts and other obligations to the State.[44] This perspective was advanced by Knapp in 1905, his agenda being to "replace the metallistic view [of money] by one founded on Political Science."[45]

Knapp wrote "the concept, means of payment, is [free] from the actual nature of the material"[46] therefore, so long "as a given material is *per se* a means of payment, money has not yet come into being"[47] He then goes on to define "a higher stage of development"[48] providing for it the name "Chartal form" leading to this tradition being subsequently defined as Chartalist.[XIX]

Following Knapp's train of thought neither the pieces themselves, nor the material they are made of, convey the property of being

[41] See Starr (2012).

[42] The emergence of a medium of exchage takes place in an environment where individuals are already exchanging goods. Money is nothing else but a commodity set in motion by the market through the mechanics of exchange.

[43] The denomination most frequently used. Perhaps worth making a clarification at this stage between barter and commodity money. Barter relates to the subjective exchange of goods between two people, whereas commodity money is a good passible of exchange without the direct subjective interest of the parties coming into play. See also Goodhart (1998).

[44] It explains why many argue the State has to keep a monopoly as the only mechanism that could ensure an upper bound over issuance. As Friedman noted "[c]ompetition... is inappropriate for determining the amount of fiat currency" (see Friedman 1951, p. 211). Seigniorage, in turn, is the way by which State monopoly is expressed.

[45] See Knapp (1924, preface: viii). His work was originally published in German in 1905. Although reviewed for the *Economic Journal* by Sanger in 1906, it found a wider audience when the Royal Economic Society (induced by a 1922 article by Bonar appeared in the *Economic Journal* on Knapp's 3rd edition) promoted the translation into English, published in 1924.

[46] Ibid., p. 25.

[47] Ibid., pp. 25-26.

[48] Ibid., p. 26.

chartal.[49] That property is always "associated with the State which introduces it"[50] in the sense that it is "a creation of law"[51] For this theory to be complete an additional yet key question needs to be answered. If, according to Knapp, money is a "Chartal means of payment"[52] that is not intrinsically valuable[53] because its material content is not essential for establishing its validity, then why people would generally accept it as means of payment? The decisive element in Knapp's theory is not issuance, but acceptance by the State. In other words, to understand what constitutes money (and, perhaps, nothing else) one has to view it as a key component of the social contract.[54]

As Wray[55] has put it,

> "Taxes drive money": if a sovereign has the power to impose and enforce a tax liability, it can ensure a demand for its currency.[56]

Money is therefore unique in that it provides a "service" to discharge obligations with the State.[57] Furthermore, in order to play such role it is argued the monopoly over its issuance should be in hands of the State, as a necessary condition.[XXI]

[49] See also Wray (1998, pp. 23-29).

[50] This has led this school of thought to be also known as "State money approach." That said, as it will be discussed later in Section 4 concerning money as an institution, it remains unclear how the social construction of money "by means of authority" would take place, or equivalently, the meaning of a State in such case.

[51] See Knapp (op.cit., p. 40).

[52] Ibid., p. 42.

[53] Assumed to be valuable: this qualification (not made explicit) is key, if value is believed to be ultimately driven by perceptions. Paraphrasing Tobin (1996, ch. 5) money has value because members of a society agree that it has value.

[54] The notion of "civil society" as in, e.g. Ehremberg (1999) or Kaviraj and Khilnani (2001), could be equally used here as a replacement of the notion of State.

[55] Perhaps one of the clearest exponents of what is defined as Neo-Chartalism.

[56] In Wray (op.cit., p. 51). The application of this precept can be traced as far back as Ptolemaic Egypt, for example, leading some scholars to conclude that "[the] economic power of the state is historically the crucial element in the history of monetization and, as the Ptolemaic case shows, state power to demand taxes in coin and payments into state banks were keys to the process." See Manning (2006, p. 27).

So much so that A. Smith made precisely the same point, when stating that "[a] prince, who should enact that a certain proportion of his taxes should be paid in a paper money of a certain kind, might thereby give a certain value to this paper money." In A. Smith (op.cit., book II, ch. II, p. 145).

[57] This principle even stood through hyperinflationary episodes. The only departure is that, in a hyperinflation, people repudiate local money for the settlement of private debts but the means for servicing fiscal obligations does not (usually) change. Such repudiation gets materialised as a flight to foreign-denominated currencies that assume the role of an asset, a means to store value (as trust shifts away from local government) rather than becoming a medium of exchange despite them becoming highly liquid.[XX]

There are additional views on money, of course. For example those of Simmel and his approach to it from a sociological perspective. Simmel's work, built around his notion of *Sociation*, is considered by many to be another exponent of the Austrian School.[XXII]

Simmel wrote that

> one should properly speak, not of society, but of sociation. Society merely is the name for a number of individuals, connected by interaction. It is because of their interaction that they are a unit – just as a system of bodily masses is a unit whose reciprocal effects wholly determine their mutual behavior... society certainly is not a "substance," nothing concrete, but an *event*: it is the function of receiving and effecting the fate and development of one individual by the other.[58]

Simmel's discussion of money and of economics is only a backdrop to his main agenda: an attempt to investigate modernity.[59] Nevertheless, he makes some influential contributions.

In his study of economic phenomena, Simmel considers exchange to be essential. It is the mechanism that allows the individual's desires to be expressed effectively, transforming the subjectivity inherent to the way individuals relate to physical objects into "an objective, supra-personal relationship between objects."[60] To Simmel, it is through exchange that a society is established, not the other way around.

> The exchange of the products of labour, or of any other possessions, is obviously one of the purest and most primitive forms of human socialization; not in the sense that 'society' already existed and then brought about acts of exchange but, on the contrary, that exchange is one of the functions that creates an inner bond between men –a society, in place of a mere collection of individuals.[61]

[58] Simmel, in Wolff (1950, pp. 10-11).
[59] In his words, to investigate "the inner meaning of specifically modern life and its products, into the soul of the cultural body." (1903, p. 120)
[60] See Simmel (op.cit., p. 83; underlined mine).
[61] Ibid., p. 187.

He then conceives the monetary system as the unintended result of social evolution rather than a conscious creation by a political entity.[62] In such system, money derives value not only as a medium of exchange[63] but, on occasions, also "as the object of a transaction sufficient to itself."[64] For money to be accepted in exchange it requires trust among individuals, trust that does not depend (in contrast to Knapp) upon guarantees by a central public authority as prerequisite.

> Without the general trust that people have in each other, society itself would disintegrate... [in] the same way, money transactions would collapse without trust.[65]

Simmel argues that divisibility is a key quality that might determine why a particular commodity might be chosen, over all others, for exchange. Money "is that divisible object of exchange, the unit of which is commensurable with the value of every indivisible object"[66] adding that "it could not have developed as a means of exchange... unless its material substance had been experienced as immediately valuable"[67]

Could that explain why precious metals such as gold and silver have been used as money?[68] Not quite, at least to Simmel.

---

[62] The work by Parry and Bloch, on the contrary, suggests that "an existing world view [is what] gives rise to particular ways of representing money" (1996, p. 19). This conception of money as a social relation is present in Ingham, when he argues that money is "a system of social relations based on power relations and social norms" (2000, p. 19). A perspective akin to that of Harrod, who wrote "[m]oney is a social phenomenon, and many of its current features depend on what people think it is or ought to be" (1969, x).

[63] See Simmel (op.cit., pp. 356-357).

[64] Instances when money "has suspended its qualities as a means, but also in the sense that it is, from the outset, the self-sufficient centre of interest, which also develops its own distinctive norms and, at the same time, completely autonomous qualities and a corresponding technique."(ibid., p. 333)

[65] Ibid., p. 191.

[66] Ibid., p. 136.

[67] Ibid., p. 152.

[68] At this stage, many see Simmel joining the Metallist camp. As Einzig (1966) has noted, Metallism can also be used to refer to other non-metallic commodities that play the role of money. Because the more developed versions of commodity currencies have generally involved gold or silver, associating Metallism *de facto* to precious metals is, somehow, understandable.

In his view, "as soon as [any commodity] is used in the same manner as the value that it buys, it ceases to be money" and perhaps more importantly, he argued that

> [if] it is claimed that the value of money consists in the value of its material, this means that its value is embodied in the qualities or powers of the substance which are not those of money... money does not necessarily have to be based upon substances that are intrinsically valuable, i.e. valuable in some other respect. It is sufficient if the ability to function as money is transferred to any substance, the other qualities of which are quite irrelevant.[69]

Hence "money can be only money and nothing but money"[70] or as Iwai has more recently defined it, "money is money simply because it is used as money."[71]

Soon enough, the historical and anthropological schools began to challenge the belief that money originated from the inconveniences of barter. This is not equivalent, however, to saying that money did not arise from a process of exchange. By the same token, and as Simmel had done in some way, the traditional anthropological perspective [XXIV] assumed money was akin to "a thing created through commodification, [that] carries with it categorical information about itself and does not require contextualisation beyond its evaluation in relation to similar entities."[72]

Hutchinson argues such approach "is premised on the idea that 'things-in-themselves,' rather than the social relations through which they flow, differentiate 'spheres of exchange'"[73] The question is not quite about how the circulating objects might create separate exchange spheres but rather about how people circulate their "knowledge" about exchanges (e.g., market and kinship relations) leading to the emergence of distinct boundaries between them.

An additional important contribution from the anthropological camp has been the study of the gift system,[74] and the implication that money originated from other transaction mechanisms than commercial exchange. The give and take of gifting –the acts of giving,

[69] See Simmel (op.cit., p. 163). George Berkeley took a similar view, long before Simmel.[XXIII]

[70] Ibid., p. 163.

[71] In Iwai (2013, p. 398). Interesting to note that despite the very similar phrasing, Iwai seems to be completely unaware of Simmel.

[72] See Strathern (2005, p. 124).

[73] See Hutchinson (1996, p. 90). She describes how money originating from work, say, was not equivalent to money coming from the sale of cattle to the Nuer people of South Sudan. In other words, money in itself is not enough to differentiate between social relations. The emergence of such categories suggests the spheres of exchange outlined by Bohannan (see note XXII) are not as clear-cut as otherwise presumed.

[74] Its theoretical foundations first laid down by Mauss (2002 [1954]).

receiving and returning– is both complex and diverse, and its economic implications are far-reaching. In his study of the Melanesian society, Malinowski concluded[75] that it was based on the principle of reciprocity[76] and this, immediately, introduces some complications. That the items transacted "are like or unlike" is not of the essence; the "perceived parity between the transactors" is.[77] The question then becomes "not how many ones make up 20 or 30 or whatever, but how many ones make up (the right) one."[78]

In the characterisation of the gift system provided above, the word *commodity* suddenly dissapeared. Indeed, commodities and gifts traditionally represent two different realities for social anthropology. Mauss postulated that "[gift] objects are never completely separated from the men who exchange them"[79] in contrast to commodities, as they do not transfer the giver's "identity" to the buyer. Commodities, however, can also be carriers of meaning (e.g. conveying a "membership" to certain group, in the sense of projecting aspirational elements that are knitted into social identity). Gift and commodity can become interchangeable, under certain conditions.[80]

In the chapter analysing pre-currency stages and the discussion of the mechanics of gifting and trading in Papua, Quiggin makes

[75] As a critique "the spirit of the gift" that Mauss identified as the driving force behind the act of returning. As Mauss delved into the Maori law, he wrote

> [in] this system... one must give back to another person what is really part and parcel of his nature and substance, because to accept something from somebody is to accept some part of his spiritual essence, of his soul. (op.cit., p. 16)

[76] The binding force of every economic transaction therefore lies in the sanction(s) that either side may raise to break the bonds of reciprocity. See also Kranton (1996).

[77] See Strathern (in Humphrey and Hugh-Jones 1992, p. 186). She adds "[items] in themselves... carry no guarantee of equivalence, not even two identical looking pigs. For in terms of particular social relations... no two things are qualitatively equivalent" (ibid., p. 187). This somehow contrasts the perspective set forth by Gregory (1982) suggesting that in gift-exchanges intervening parties present each other with goods or services that are basically alike so to reinforce the social bond between them.

[78] Strathern (op.cit., p. 187). Despite focusing her research on the mechanics of barter between Nepalese communities, Humphrey (1992) points towards the moral commitment embodied in each transaction as defining a notion of "equivalent value," in essence what Strathern is describing.

From a barter perspective, this is reflected in what counts as a "fair price" (that is, the exchange rate between commodities bartered; see also Sahlins 1972).

[79] Mauss (op.cit., p. 31.)

[80] See, e.g. Godelier (1977), Parry and Bloch (1996) or Carrier (1991).

an interesting observation.

> When arm-rings are too small to be worn, but have definite equivalent values in sago; when the overgrown axe-blades are exchanged for pigs, canoes and ornaments; when the shell-disks, made only in certain districts, are made up into strings, and one string will buy a dozen pots; then currency is establishing itself, and these special objects, becoming more specialized and unfit for domestic use, are acquiring the token characters that we recognize in money.[81]

Bourdieu, however, suggests the time lapse between the stages of giving and returning is the unique factor differentiating gift from barter.[82] Graeber notes that Bourdieu always considers gifts as "part of a game of dominance, an attempt to accumulate symbolic capital and gain an advantage over the other party."[83] Following this logic, if the time lapsed between the acts of receiving and returning shrinks to zero then gifting becomes analogous to barter.

To conclude this overview, other scholars point towards the role of credit systems as precursors to money. Commenting on the usage of barter by the communities of framework knitters in 19th century England, Quiggin suggests that "[such] inconveniences are avoided in simpler societies by elaborate customs of credit, deferred payments or payment by services"[84] hence pointing towards credit being a precursor of monetary or other arrangements.

Along that line of argumentation, Einzig notes that "[it] seems probable that a credit system developed in Greece as in other parts of the ancient world long before the adoption of coinage."[85] There are indications of the routine practice of consolidating and discharging obligations through paper transactions or book-keeping[86] in pre-Ptolemain Egypt, seemingly propelled by the shortage of coinage

[81] See Quiggin (1949, p. 19).
[82] Based on his study of the Kabyle in Algeria; in Bourdieu (1979).
[83] So, ultimately, "it is a matter of self-interested calculation" (see Graeber 2001, pp. 28-29).
[84] See Quiggin (op.cit., p. 5).
[85] See Einzig (1966 [1948], p. 225). He subsequently adds "for this reason the view taken by Zimmern [1922] that the adoption of coinage made a fundamental difference to Greek economic and social life... is probably exaggerated" (also see endnote XII for a counterargument). Einzig makes it clear his research program is about "laying stress on the non-commercial origin of money and on the possibility of the existence of credit before money, of money before barter and of barter before private property or division of labour" (ibid., xvi).
[86] That is, payments settled on account.

in the Egyptian countryside.[87] The factual evidence is been somewhat disputed. Kim notes, however, that

> coinage was probably not in itself responsible for the substantive changes in social relationships apparent during the archaic period... simply appears much too late for it to take the credit.[88]

In any case, this idea of credit arrangements taking precedence over money has in A. Mitchell Innes perhaps one of its most notable proposers.[XXV]

To Innes, money evolved not from a pre-money economy but rather from the credit and debt relations emerging from the mechanism of tribal *Wergild* designed to prevent blood feuds.[89] On the subject, Grierson wrote

> [the] conditions under which these laws were put together would appear to satisfy much better than the market mechanism, the prerequisites for the establishment of a monetary system. The tariffs for damages were established... [and] since what is laid down consists of evaluations of injuries, not evaluation of commodities, the conceptual difficulty for appraising unrelated objects is avoided.[90]

It can be easily seen that this system does not require the pre-existence of markets, but an authority to levy such obligations, name the things needed to satisfy those obligations, and eventually issue the things accepted as payment.[91] One of such "things" was, indeed, money.[92]

[87] See Von Reden (in Meadows, eds., 2001). The evidence presented by Von Reden relates to registers on papyri that pertain to debts, deferrals of payment, debt consolidation and discharging. Kroll (2012) however dismisses the case for shortage of coinage to be the cause behind the use of credit. See also Bleiberg (2002).

[88] See Kim (in Cartledge, Cohen and Foxhall eds., 2002, p. 49).

[89] The *Wergild* or "man payment" was a compensation paid to the injured party (or, in case of death, to his family) by the offending party or his family. It was a system to "make ammends" that became established by tradition, its most developed version being the *Leges Barbarorum*, the laws of the Germanic tribes that settled along the frontiers of the Roman Empire from 400 AD.

The amount of the penalty fluctuated greatly, based on the severity of the crime, the wealth or social class of the victim, the evaluation of the damages and the ways in which those were assessed. Lists of fines for each possible transgression were developed and a designated "rememberer" was responsible for passing it down to the next generation.

[90] See Grierson (1978, p. 13).

[91] By denominating those goods that could be delivered for settlement of an offense, the authority exercised its rule through price fixing.

[92] Once again, the material of which money was made had no relevance as long as its nominal value was set by authority.

Perhaps more importantly, Innes reasoned the market is nothing but a clearinghouse for debts and credits, placing trade (exchanges) as a subsidiary phenomena.[93] Money, then, is not a relation-free product but a social phenomena. As a corollary, money is not seen anymore a medium used primarily to "lubricate" exchanges.

Having reached this stage, do the competing theories presented above provide a clear (and substantiated) enough characterisation of what is money? The next section briefly discusses this topic.

4. What is money?

[Everyone] can "create" money–the only problem for the creator being to get it "accepted."
H. Minsky, 2008, p. 79

Up to this point, the discussion has mostly pivoted around an exposition of the origin of money, touching on its most frequently assigned function: that of being a medium of exchange. Some see it as a medium that primarily helps eliminate trade frictions; to others, it has the role of a "social lubricant" being used "for almost anything but trade."[94]

The opening quote from Minsky makes it palpable that creating money, or something that resembles money by writing "this is worth 10 dollars" on a piece of paper, is not the issue; rather, how to get another person to accept such an instrument, without being compelled to do so, as settlement of an obligation.

The usual way to define money is through the functions it provides. Jevons (1919) suggested money has four distinctive roles, outlined below.[95]

- A medium of exchange;
- A common measure of value;
- A standard of value; and
- A store of value.

Nowadays, the first attribute is typically rephrased as medium of exchange or payment (some authors, however, separate the exchange from the payment spheres); the second attribute is that of being a unit of

[93] One of the ways an individual becomes a creditor or a debtor.
[94] See Graeber (op.cit., p. 130).
[95] See Jevons (op.cit., ch. III).

account or *numeraire*; the third attribute gets fused to the first one, so it does not appear separately; and the last one remains the same.

Irving Fisher, however, took a further step by postulating a much narrower definition of money. To him,

> [a]ny property right which is generally acceptable in exchange may be called "money." Its printed evidence is also called money[96]

adding that, what separates money from other goods is basically

> [t]he facility with which it may thus be exchanged, or its general acceptability, is its distinguishing characteristic... [a]ll that is necessary in order that any good may be money is that general acceptability attach to it.[97]

Brunner followed this last train of thought in one of his contributions to the *New Palgrave*, supporting the view of money being a medium of exchange before anything else.

> Money is still best defined in the classical tradition to refer to any object generally accepted and used as a medium of exchange. Financial innovations associated with technological or institutional changes do not modify this definition.[98]

a perspective also echoed, e.g. by Tobin.[99]

Others, however, take an different stance. That is the case of the Institutionalist School[XXVI] of which Ingham, a leading figure in economic sociology, is perhaps its most known contemporary exponent.[100] To them, being a unit of account is the key role in monetary relations, as opposed to the quality of being a medium of exchange.[101]

[96] See Fisher (1920, p. 5). Recall here our previous discussion about Cicero's characterisation of *currency* in p. 7.

[97] Ibid., p. 8. Fisher also made clear, in passing, that acceptability may be reinforced by law, but that "such reinforcement is not essential."

[98] See Brunner (in Eatwell, Milgate and Newman eds., 1989, p. 263; underlined mine).

[99] Comparing the different attributes typically assigned to money, Tobin wrote that "[m]oney is the principal means of payment of a society, but it is only one of many stores of value" adding, in passing, "and quantitatively a minor one at that." In Tobin (1996, p. 143).

[100] See, e.g. Ingham (1996, 2004) for a discussion.

[101] Henry (2002) mentions that in Egypt, at some point during the Old Kingdom, a specific unit of account (the *deben*, equal to 92 grams) was introduced "to maintain records of obligations and the extinguishing of those obligations" using some form of book-keeping, adding that "[m]oney [had] no value in and of itself."

As Ingham himself emphasised,

> [a] 'monetary space' is defined by money of account in terms of which debts are contracted and discharged and all transactions are conducted.[102]

First and foremost, then, money is a measure of "abstract value"[103] and only then becomes a means for transporting and storing[104] this abstract value.[105]

Still, taking a step further in the direction of considering money a medium of exchange, nearly a generation ago Kocherlakota presented the thought-provoking suggestion that money, assumed as a coordination game,[XXVII] is ultimately "memory."[106] To do so, Kocherlakota first defined an economy where agents are matched, engage in trade, and memory is the knowledge of the past history of an agent's trading partners and of all the agents that were directly or indirectly in contact with them. Consequently, memory is nothing else but a technology revealing the complete history of agents in any pairwise match.[107] In principle, under perfect monitoring[108] money becomes a

[102] See Ingham (2004, p. 71; underlined mine)

[103] Such abstract value is what defines the "money of account" attribute; see Ingham (ibid., p. 70).

[104] For final payment or discharge of debts.

[105] Ingham reaches the conclusion that being a "[m]oney of account is logically anterior to any form of money that bears the abstract value" and following Hicks (1989) asserts "all the other functions [of money] –medium of exchange, for example– may be subsumed under these two attributes." See Ingham (ibid.; underlined mine).

[106] See Kocherlakota (1998; 2002) and related papers. Nearly a decade before Kocharlekota, Giddens (1990, p. 25) had already made the argument that "money is independent of the means whereby it is represented, taking the form of pure information." But it was Niehans in his *Theory of Money* who had already floated the (related) idea that money does not need to take the form of tangible, physical money objects. He wrote

> Exchange is a way to make sure that nobody can escape his budget constraint(s). If one could be perfectly certain that everybody always stays within his budget constraint, everybody could be allowed to obtain goods without a specific *quid pro quo*.

See Niehans (1978, p. 62).

[107] By now, a well-established mechanism to motivate the existence of frictions due to, e.g. information asymmetry, is by modeling trade as occurring in small groups, often pairwise matches. It is then assumed that some "technology" is available (Kocherlakota uses "enforcement" but it is not the only possible one) to select agents from the population and match them together.

[108] In other words, that some form of book-keeping is in place that tracks the ownership of assets arising from every trade (and makes this knowledge public, so there is complete observation).

primitive form of memory: any allocation that could be achieved with money could also be achieved with memory.[XXVIII]

As long as there are no disputes amongst agents memory can indeed susbtitute money; but equally so, memory is distributed among economic agents that potentially have conflicting interests.[109] That brings us back to the issue of trust.[110] Shubik once aptly noted that "cash leaves no paper trail."[111] In an cashless economy only supported by memory, transactions would only be possible if records are kept that can be accessed and validated retrospectively.[112]

To recap, although there is good agreement on the multiple roles of money, defining its primary role remains a largely unsolved question.[113] There are three distinctive camps in this lively debate.

- Those focused on understanding how come assets having no intrinsic value, such as fiat (paper) money, are however routinely perceived (and hence used) by economic agents as a storage of value;
- Those that instead concentrate on money's role as a medium of exchange and the fact that, as such, it must also be a store of value;[114]
- Those looking at how money operates in environments of decentralised price formation between buyers and sellers, that is, money's role as unit of account in the decision-making process.

Underlying the above is the additional debate about the frictions (or impediments, more colloquially) that led to the appearance of money

[109] Otherwise known as the "coarsening" of information. The idea that less information can make agents better off has been recognized at least since Hirshleifer (1971).

In the real world, where trade is dominated by impersonal relationships rather than personal ones, it becomes difficult to deter opportunistic behavior, as Bigoni *el al.* (2015) emphasise. They furthermore demonstrate, in an experimental environment, that "the suggested theoretical affinity between money and memory does not empirically translate into a functional equality" reinforcing the view that "monetary systems are key to support impersonal exchange, intertemporal trade and, consequently, large-scale cooperation."

[110] There are formal models of trust available; for some considerations, however in a completely different context, see Salazar (2015). Link is https://bit.ly/2Gr98vx.

[111] See Shubik (1999, vol. I, p. 236).

[112] That is the job of memory in Kocherlakota's setup.

[113] Or a question whose answers are (sometimes quite vocally) in conflict.

[114] Because the converse does not hold (clearly, not every store of value is a medium of exchange) the question to solve, then, is how goods used as stores of value ended-up being a medium of exchange.

in a modern economy,[115] how money is valued in equilibrium and the mechanics by which money is exchanged for goods.

To sum up, if there is anything clear so far is that physical form does not define money. The ways money can be (and has been) represented are immensely varied.

5. Where do we stand?

Monetary Theory is a subject much favoured by cranks
and by visionaries... since very often the cranks
and visionaries are in sufficient control
to try out their theories.
F. Hahn, 1989, p. 5

The above discussion, if anything, has shown the complex inner workings of money, the evidence (at times conflicting) around its origin, and consequently, the multiple perspectives that over years have emerged on the basis of those facts.[116]

Such a rejoinder seems even more pertinent when looking at the narrative that pervades much of the present debate around cryptocurrencies, and talks of money in more general terms. In fact, the core Bitcoin community[117] has not been able so far to find a single, coherent framework to define what a cryptocurrency is,[118] whether it has any worth, and why it has become a necessity in current times, socially or otherwise. The economic facts and monetary history presented in the previous section, although not exhaustive, already suggest that more care should be exercised when characterising money.

[115] Part of that story has been presented in the previous section, the focus of what has been dubbed by Wallace (2010, vol. 3, ch. 1; see also Note XXVIII) as the *mechanism-design* approach to monetary theory; its precedents can be traced back to Ostroy (1973) and Townsend (1987, 1989). To reiterate, market frictions are typically assumed to involve either scarcity or asymmetry of information (or rather, imperfect monitoring); the impact of geographical separation between agents (costly connections); and imperfect recognizability of assets. Some add the existence of inadequate institutions as an additional source of frictions.

[116] By any metric our exposition so far can be considered exhaustive; this paper only scratches the surface of the topic and goes through a number of perspectives and literature using a rather broad brush.

[117] Extensible to the alt-coins community as well.

[118] Or a virtual currency, in more general terms.

For starters, a cursory review of the available research suggests the standard (or, lets say, neoclassical) explanation for the origin of money, and why a commodity becomes accepted by society as general medium of exchange[119] does not hold water. Such traditional description, inspired by Smith and later developed by Menger and Jevons, has been consistently refuted by scores of anthropologists, sociologists and historians.[120]

It is a fact that bitcoin's emulation of a precious metal[121] appeals to libertarians and anarcho-capitalists alike.[122] Those are the groups, to this day, making the core of the "cryptocurrency" community. Casual review of the posts appearing in social media platforms[123] reflect a clear antipathy towards institutions,[124] in particular central banks and the Federal Reserve, and an abundance of debates around the perils of inflation (and hyperinflation) and the benefits of a currency that is deflationary by design.[XXIX]

Much of the talk about cryptocurrencies is taking place at the fringe of economics or at the very least through a particular looking glass, driven by normative judgements concerning social dynamics and political processes.[125] The backdrop provided by debates around money shows, if anything, that there is by no means agreement on its foundations. Hence, it seems useful to make an attempt at further dissecting the logic supporting Nakamoto's predicament and by extension, of cryptocurrencies designed like bitcoin. A nearly 15 year old debate stemming from a journalistic article provides an interesting starting point.

[119] Quite clearly, a separate matter altogether.
[120] As discussed in the previous pages (and futher expanded in the Notes section) it becomes clear that, e.g. Menger completely ignored the fact that money existed for thousands of years before the emergence of market economies.
[121] See the quote by Nakamoto mentioned on p. 4 herein.
[122] Refer to Note X.
[123] Conversations taking place in specialised forums such as BitcoinTalk or Reddit; in Twitter and Telegram; blog posts in Medium and other outlets, e.g. Cointelegraph, CoinDesk and Bitcoin Magazine.
[124] Be it financial or political; in more general terns, any entity seen as a centralised instance of power.
[125] Rather than factual evidence, let alone any sort of proof related to the undelying economics.

In January 2004 Frank Shostak, from the Mises Institute, wrote a piece in the *Mises Daily*[126] in response to another article by Hal Varian published in the *New York Times* earlier that month.[127] Shostak picks on a "controversial" argument in Varian's article attempting to explain why fiat money (e.g., dollars) have any value. This is perhaps best reflected by a statement found in Varian's piece, quoted below.

> [P]aper currency can take on a life of its own, even in the absence of government backing. At the same time, it is clear that government backing makes a significant contribution to the value of paper currency.

The first part of the above quote reflects Varian's use of expectations formation as the mechanism that shapes "social convention"; in other words, "that dollar bill in your pocket"[128] is worth something because of the expectation that it will be accepted in exchange by someone else. Projected to all economic agents in society, that mutually reinforcing process is what explains why fiat money is widely accepted.[129] The second part of the quote from Varian's piece suggests that, ultimately, "money is money" mainly (if not excusively) due to the power of the State.[130]

In his answer, Shostak wrote that

> for something to be accepted as money it must have a pre-existing purchasing power, a price[†]... [by] regressing through time we will eventually arrive at a point in time when money was just an ordinary commodity where demand and supply set its price. The commodity had an exchange value in terms of other commodities, i.e., its exchange value was established in barter. To put it simply, on the day a commodity becomes money it already has an established purchasing power or price in terms of other goods.[131]

---

[126] See https://bit.ly/2IQN0Z8.

[127] See https://bit.ly/2IRiCOs. Hal Varian is currently chief economist at Google.

[128] Ibid.

[129] A sort-of "money is accepted because it is accepted" type of logic. Here, Varian appeals to what is known as "network effects" or a situation wherein the value of an object is dependent on its rate of adoption; note, however, this concept has been mostly used to describe technology adoption which is a rather different kind of fish.

[130] Varian does not quite make a *de jure* argumentation *a la* Knapp but more about the adoption of sound policies by the State to preserve the value of the fiat money it issues. Despite all the legal tender laws in the world, if people don't see that transacting in a certain currency is in their best interest, nothing will force them (bar certain unavoidable exceptions) to do so. See also footnote 50.

[131] Shostak (op.cit.; underlined mine).[†] Given Shostak's attempt at explaining how money emerged as medium of exchange, his argument still goes back to a commodity being first accepted as unit of account. Refer to the discussion in Section 3, p. 9.

Key to Shostak's argument is the so-called "regression theorem" by von Mises. It's not a formal theorem but the enunciation of a principle outlined in his 1912 book *Theory of Money and Credit* stating that

> [o]nce an exchange ratio between money and commodities has been established in the market, it continues to exercise an influence beyond the period during which it is maintained; it provides the basis for the further valuation of money. Thus the past objective exchange value of money has a certain significance for its present and future valuation. The money prices of today are linked with those of yesterday and before, and with those of tomorrow and after.[132]

Frank Hahn provided, as was customary in him, an elegant criticism of this principle.[133] Starting from Radner's formalisation of the sequence economy[134] and the role played by expectations,[XXX] Hahn made the argument below.

> Suppose that, in the first instance, we think of such a sequence economy in rational expectations equilibrium. A problem arises if we model such an economy as being of finite duration. If there is a last date, then clearly at that date no agent will wish to hold paper money[‡] –it must be worthless. But this, under rational expectations, is known to agents at the moment preceding the final date. If they hold money to transfer to the final date, they will be forgoing current consumption for no future benefit. So no one will wish to hold paper money at the moment preceding the final date, and it will thus also be worthless at that moment.[135]

[132] See von Mises (1981 [1934], II.8.4; underlined mine). This formulation is akin to a backward-looking expectations formation hypothesis. In essence, the value of an asset accepted in exchange is contingent on its previous value. Rothbard (1976, pp. 169) argued also that

> the demand of money can be pushed to the last day of barter, at which point the temporal element in the demand for the money commodity disappears, and the causal forces in the current demand and purchasing power of money are fully and completely explained.

immediately adding

> Mises [via the regression theorem] demostrated that Carl Menger's historical insight into the way in which money arose on the market was not simply a historical summary but a theoretical necessity. (ibid.)

Be that as it may, Hicks took a swipe at von Mises, saying he regarded money as a "ghost of gold" (Hicks 1967 [1935], p. 62). Recall gold and silver are considered typical examples of "pure commodity" money.

[133] Hicks was not alone. Patinkin (1965 [1956], pp. 115-116) also had a go at Mises.

[134] In Radner (1972). In a sequence economy *a la* Radner "we must take note that agents will act today in the light of their expectations of the prices at which they can transact at future dates. That is an ominous departure from the complete market idealisation." See Hahn (ibid., p. 8).

[135] In Hahn (1973, pp. 4-5; underlined mine). [‡]Hahn talks here about fiat money, precisely the context of the Varian-Shostak debate.

Although Varian does not properly explain why fiat money can have any value now, regardless of whether it might once have had value, von Mises' logic seemingly fails to explain why it might retain value in the future. Hahn made the case for expectations as a key driver of value. His argument was that if the world would eventually "come to an end" –a finite duration economy– then at that point, assuming rationality, it is unlikely anyone would be willing to accept paper money[136] as there will be no one left with whom to exchange it.[137]

By the same token, if there will be a time in the future when paper money will lose all of its value because no one will accept it, then a straightfoward application of von Mises' backward unravelling implies that it should command no value now. If paper money is currently valueless, then, proceeding backwards in the same way, it had no value originally.[138]

Hahn's train of thought[XXXI] immediately begs the following question: if not from a commodity, where does money derive its value from?

[136] Or any form of money for that matter, even if money has an objective-use value determined by the service it could provide in non-monetary terms (e.g. a precious metal that could be melted and converted, say, to jewelry).

[137] Cass and Shell, however, considered indefinite future as a pre-requisite for modelling money. They wrote that if

> [a]t the end of the last period, money is worthless... in the next-to-last period, all individuals desire to dispose of money holdings in order to avoid capital losses. This drives the price of money to zero at the end of the next-to-last period. And so on. Individuals with foresight, not wanting to be stuck with the monetary 'hot potato', thus drive the price of money to zero in each period. See Cass and Shell (1980, p. 252).

Hahn mocked this argument: "as I understand it" he wrote, "the laws of physics provide an absolutely certain upper bound on the life of the solar system" leading a useful abstraction such as rational expectations being driven to an "absurd conclusion." See Hahn (ibid.)

[138] In the sense of value derived from a commodity, as implied by Menger. If the value of fiat money in terms of output is zero, then the demand for money is undetermined. Let's say P denotes the money price of goods. Clearly, one unit of money purchases $1/P$ units of goods. For $1/P > 0$ one can easily see that $0 < P < \infty$.

One experiment that looked at backward induction "in operation" is McCabe (1989) using money-like tickets resembling fiat money. Contrary to the theoretical outcome in an economy with known finite end, McCabe found the tickets were still accepted by the game players. He then concluded that home-grown priors as to the acceptance of money in everyday life situations led to such result. A different explanation is offered here.

He provided an answer that hinges upon the existence of transaction costs.

> Provided search costs are positive one can show that all players [in an exchange game] will be worse off in that situation than they are in the monetary equilibrium. To go from a barter to a monetary equilibrium would require co-operation, and this, one might speculate, is why governments play a large role in monetary matters.[139]

There are indeed other ways of thinking about the issue. It could be argued that agents are not concerned about the last date in their lives, as Hahn suggested; they only care about the "practical" time horizon (whatever that happens to be) when forming expectations.[140] By applying Hahn's logic, if the end of an exchange sequence[141] is beyond the time horizon defining the relevant "decision making frame" of economic agents, then it should have no impact on the agent's actions.[142]

This argument has some interesting implications. Suppose now that agents have disparate beliefs (due, e.g. to information asymmetries) about the death knell for fiat money. In the presence of uncertainty driven by heterogeneous beliefs some agents, perhaps, might be prepared to exchange something of value for a piece of paper that others believe to become useless in a soon-to-be date.[143] If money

[139] See Hahn (1989, p. 11). He argues "those costs may take the form of uncertainty of finding a buyer" for assets in barter exchange; see Hahn (1973; 1981, p. 27).

[140] The use of the word "practical" only emphasises the fact that a time horizon has to be relevant given the decision(s) agents are facing. There is also the rather obvious fact that real-life agents have finite life expectancies.

Sociologists Carruthers and Babb argued "[m]oney's effectiveness depends on people's expectations... as such, people's response to it is determined by what they collectively think everyone else's response will be." They subsequently added "[w]hen money is problematic because of a changing or highly uncertain value, exchange becomes more difficult, and people may revert to barter." (Underlined mine.) See Carruthers and Babb (1996, p. 1557). Incidentally, that is precisely what happened in Argentina during the immediate aftermath of the 2001 crisis; see, e.g. Lacoste (2003) and Gomez (2009, ch. 6).

[141] The equivalent of a "final date" stated by Hahn (ibid.)

[142] That something will come to an end does not imply a constraint unless that "end" is expected to happen soon enough to alter expectations, and hence influence immediate actions. In theory, the only consequence is that it imposes a constraint on the search space for trading partners, as exchanges would only be possible between individuals whose decision frame is not impacted by the prevailing belief.

[143] It does not mean that agents do not realise its value will come to zero at some (undetermined) future time, only that such date is not relevant in their decision-making process.

is assumed to be a coordination game[144] that means the game has a random stopping time.[145] In such scenario, fiat money can retain positive value for some agents, at least for some time.[146]

Note, however, the backward induction logic breaks down once again.[147] The question about how asymmetry in beliefs leads to fiat money having a positive value has not been fully answered yet, but one alternative explanation is inertia.[148] It is not unconceivable that could be the case.

The other route for explaining why fiat money retains a positive value, as outlined by Knapp and others, is that money does indeed provide a distinctive real service rather than value being the result of inertia, speculation[149] or even irrationality. A service that, once again, hinges on the possibility that economic agents have for using fiat currency, and only fiat currency, to discharge their fiscal obligations. Something that was also raised by Wicksteed, whose doctrinary alignment was "practically that of Wieser and the present-day Austrians"

[144] A game having two or more Nash equilibria that takes place when all players choose the same strategy. So, let's say an individual accepts a familiar type of money today, relative to other trading options (e.g., barter) because he experienced that type of money was widely accepted yesterday. The other agents he trades with know that he knows that. Therefore, unless there is a signal to the contrary he expects that same type of money to be accepted tomorrow; there is no reason for repudiation before others do, and everybody else in the game thinks the same. In a way it reflects what Friedman and Schwarz observed, that "each [agent] accepts [a piece of paper as money] because he is confident others will." (in Friedman and Schwarz 1963, p. 696). Given such scenario, fiat money can be deemed to be an equilibrium in a coordination game.

[145] Formally, in a random (that is, probabilistic) stopping scenario agents do not know how many "repeats" of the game will take place. Enough uncertainty built into a finitely repeated game is equivalent to the equilibria achieved in an infinitely repeated game.

[146] This opens an interesting front: the possibility that money could still hold value regardless of buttressing by the State, as suggested by Knapp and others.

[147] Backward induction does not work if the terminal date is unknown.

[148] The inertia hypothesis was prepounded by Yaeger. He wrote "[w]ith money as with language, inertia tends to perpetuate an entrenched use." See Yaeger (1982, p. 238). Inertia could as well encompass "institutional" inertia, many times a key ingredient that hampers the objectives of stabilisation policies aimed at preventing inflationary episodes from turning into hyperinflations.

[149] The concept of *speculative behavior* outlined by Duffy and Ochs, when stating that "accepting a *token* object with consumption good to any individual *is inherently an act of speculation*." See Duffy and Ochs (1999; 2002, p. 639; emphasised in the original). They ran a series of monetary experiments having speculation as a possible, and rational, outcome. They found, however, the experimental subjects had difficulties coordinating on the speculative equilibrium, and that speculation did not take place as much as expected.

as Frank Knight cared to say.[150] In his book *The Common Sense of Political Economy* Wicksteed wrote

> [a government] by enacting that its paper shall be received in payment of all debts and obligations it can cause all the business transactions of the country to be conducted by its means.[151]

The point to be stressed here is that acceptability of fiat money for payment of taxes provides a source of non-monetary value.[152] That uniqueness, acquired through enforcement by the State, becomes a necessary condition for fiat money to retain positive value[153] and yet, as already discussed and despite its appeal, it is not the only possible explanation.[154]

Having come to this stage, the next section quickly reviews some modern variations of the theory of money, focusing on specific cases as they are relevant to cryptocurrencies.

6. New models of money

If we could let go of our faith in money,
who knows what we might put in its place?
L. Lapham, 1988, p. 237

Summing up, providing a satisfactory solution to the "Hahn Problem"[155] has been one of the biggest challenges in economic theory, focused, to a great extent, at (convincingly) answering what Hellwig stated as Hahn's

> Problem 0 – Why does fiat money have a positive value in exchange against goods and services even though it is not intrinsically useful?[156]

The genealogy of the debate around this question, so far, can be split into three. Firstly, those who believe the value of fiat money depends

[150] See Knight (1934, p. 661).
[151] See Wicksteed (1957, vol. II, ch. VII, p. 613 and ss.).
[152] Taxes, as part of the social contract, underpin peoples' position as citizens in a society; the "mandate" element stressed here. From there onwards, whether a particular level of tax pressure, or tax structure, is deemed fair (a key topic in the agenda of many political groups supporting cryptocurrencies) is a separate question.
[153] Or as F. A. Walker concluded, "[m]oney is that money does." See Walker (1878, p. 405). Also see Note XXI.
[154] See footnote 117. It cannot be denied the State can provide good enough anchors, be it by requiring taxes are paid in (its own-issued) fiat money or through legal tender laws, but those anchors cannot compelety erase market forces in price formation.
[155] Refer to Note XXXI.
[156] See Hellwig (1993, p. 216) and the recap of Section 4.

mainly (or exclusively) on the intrinsic value of "something" backing it up, in other words, those who argue money's value is defined by trust.[157] Confronting this perspective are those believing that solely the authority of the sovereign or State, as represented by the "face" stamped on a coin or printed on a paper note, is what provides a fiat currency with a positive value.[158] Finally, somewhere in the middle are those proposing money to be purely a socio-cultural phenomena, arguing that very fact is the key factor that determines value.

Be that as it may, the subsequent efforts in the economics field to deliver a convincing response to this question[159] have positioned themselves, for the most part, in one or the other extreme, yet they have both pushed for micro-foundations[160] instead of pursuing solutions determined "from above" (e.g., as a policy instrument).[161]

In his seminal 1965 paper, Hahn made the case that money is "essential" if economic agents, through its use, are able to achieve allocations they cannot otherwise reach. It relies on observing three types of frictions, outlined at different points in the previous pages, but worth reiterating below.

- The existence of a double coincidence of wants problem and the (collateral) assumption that finding a partner to trade is costly, in time and resources;
- The fact that long-run commitment cannot be enforced; and
- The anonymity of agents, in other words, their trade histories not being public knowledge.

Given those three frictions in trade, money has "a role" to play. In terms of the models used in mainstream economics to "explain money"

[157] Following Menger's school of thought, although trust is also at the core of Simmel's approach to money.

[158] Which, in turn, comes from the information carried by each coin or paper note, the most salient being the ability to discharge taxes.

[159] Perhaps an interesting fact is noticing those effors actually reduce to finding a way to make that n^{th} good –money– in a Walrasian model of the economy to have a positive value; clearly, the $n-1$ remaining goods do command positive prices defined through a barter technology having no pre-defined transaction costs (although it might be an inherently costly technology, as Hahn and others have suggested, however without formal proof).

[160] That is at the core of what is defined as New Monetarism. As for microfoundations and going back to Hellwig's `Problem 0` answering the question as to why fiat money becomes the common medium of exchange is a bit more complicated. Noting "common" as key word, one suggested explanation is the existence of so-called "thick market externalities" in search models. That said, how search decisions taken in decentralized markets might be able to internalise them is not quite obvious.

[161] In that respect, Kirman observed that "the way to develop appropriate microfoundations for macroeconomics... rests in an essential way on studying the aggregate activity resulting from the direct interaction between different individuals." See Kirman (1992, p. 119).

there are competing approaches; for sake of brevity, let's mention two of those possible scenarios.

- Consider an economy populated by anonymous agents[162] that have stochastic preferences;[163] there is a unique, perishable, indivisible good traded for money[164] in a centralised market with a clearinghouse; prices are fixed and market clearing is ensured by rationing.[165] The incentive to hold money, in this scenario, is a consequence of the assumption that agents have stochastic preferences.
- Let's again assume agents are anonymous; however, they specialise in the production of an indivisible, perishable good they do not consume[166] so buyers and sellers have to be somehow brought together; but now the market is assumed decentralised,[167] hence random matching is adopted as technology for bilateral meets between agents. There is money, also assumed indivisible. The role of money here is to "smooth out" the possibility that agents might be matched to other agents that do not have "coincidence of wants."

The differences between the examples presented above[168] (both of which find a role for money, but for rather different reasons conditional, of course, on how the economy is "conceived") shows that understanding the role of money is not an easy task, by any measure. Needless to say, a proper discussion of the models in the literature (original ideas, plus their vintages and forks) is well beyond the scope of this paper.[169]

[162] More formally, a "large" or $[0, 1]$ continuum of agents.

[163] An agent might prefer to supply a service one day, and on another day to demand it.

[164] Anonymity precludes credit.

[165] Fixed prices and a non-divisible good require demand and supply to be coordinated using a non-pricing mechanism.

[166] So commodity money is ruled out by design. In the "early generation" models, agents that held money could not produce; this assumption was later relaxed.

[167] Hence, contrary to the prior case, markets are not assumed to be well organised.

[168] Note, however, both models involve matching, which is a convenient framework to motivate the existence of obstacles to trade or information flows (frictions, as said above).

[169] The interested reader can browse either Williamson and Wright (2010) or Nosal and Rocheteau (2011) for a review. The volume of literature is by now enormous. Furthermore, there are proposals that have focused on solving Hahn's Problem in its own turf, so to say. Such is the case of the "trading post" model proposed by Starr.

Therefore, the message that should stick is simple: any project looking at providing a satisfactory answer,[170] particularly in relation to the introduction of a competing currency (such as bitcoin and other virtual "currency" proposals using cryptography as key ingredient) must take a deep and hard look at the synergies between the macro and microfoundations of money and abandon, for good, the use of any easy analogies or ideology.

7. Virtual currencies: money or what?

There is nothing more difficult to plan, more uncertain of success, nor more dangerous to manage than the establishment of a new order...
N. Machiavelli, 1961 [1514], p. 27

Having arrived at this point, several questions about cryptocurrencies require an answer. Broadly speaking, tokens aiming to become digital currencies (since bitcoin appeared on stage) strive to blend the features of physical money to the (now widely accepted) convenience of electronic transactions. Could any of this new brand of virtual tokens[171] ever become money? If not, what could they become otherwise?

And also, what are they now and what for? In the end, it is not simply about trying to find or create a "role" for this new type of construct, but about understanding whether such a role conveys any meaning and delivers some form of tangible benefit, and to whom.

These are perhaps only a few, obvious questions, but they broadly span the space of positive and normative issues related to the design of an alternative means of payment. For example, could this new brand of privately-issued fiduciary tokens have any chance of success functioning alongside fiat money? If so, is price stability achievable in such an environment? Is that purely a function of the minting algorithm (and the underlying revenue, or seigniorage, model) or of competition? Even if such co-existence delivers stable prices, can a socially optimal quantity of money be obtained? Purely from a design perspective, is a commodity-backed cryptocurrency preferable to a fiduciary one? On the institutional front, should governments support cryptocurrencies, and if so for what purpose? Is it desirable that policy makers regulate cryptocurrencies, and under what conditions? Even more, do they have to support a particular "type" of cryptocurrency?

See Starr (2012) who presents, in a single volume, a compilation of his multiple papers on the subject for the past 40 years.

[170] By that meaning workable.

[171] So not just Bitcoin but Litecoin, Ethereum, Monero or Ripple. Cryptography is used to create and enforce computational integrity, an all-important feature for any highly (or extremely) distributed and decentralised system.

Let's proceed by steps, first untangling the question of whether digital tokens can be deemed a "currency" or not, something for which the discussion advanced in Section 2 provides some cues. The answer is not straightforward because it depends on how the sphere of circulation is defined; meaning both the distribution of, and the underlying links between, economic activities[172] making use of those virtual tokens. For example, a virtual token used for trade in a given town (e.g., from buying groceries or a newspaper to paying for parking) could become a currency in that specific locality.[173] If those tokens are otherwise used to trade on a specific type of goods or services, they might become a currency in relation to exchanges involving only those goods or services (so not able to be used in exchange of other goods or services) irrespective of physical proximity.

The above requires some further qualification around the notion of "general acceptance" mentioned in Section 2. In the former case, the token is assumed to be used for payment by people in a particular town; hence the token is generally accepted, but only there. The latter case depicts acceptance by everyone (not making any distinction, e.g. by the distance between trading partners) in the space of trades involving a particular type of economic good or service.

Going a step further, what does it mean here to be "general"?[174] Probably, the answer can be more easily found by posing the alternative question, what does not being general mean? To date, virtual tokens (of which the original Bitcoin nowadays accounts for roughly 45% of the market capitalisation[175]) are all seemingly trapped

[172] This does not necessarily relate to physical proximity (or spatial distribution) although it is one consideration.

[173] There are multiple cases of companies "owning" an entire town and paying their workers in scrip (paper notes or metallic tokens, resembling coins) redeemable at the company stores, an arrangement known as *truck system*; see, e.g. Hardy (2010). Closer in time, the BerkShares are an example of privately issued scrip launched in 2006 and circulating in the Berkshire region in Massachusetts; see https://bit.ly/2Jv9oYw. There are also the REKA checks issued by the Swiss Travel Fund (REKA) Cooperative, usually given as a fringe benefit to employees at a discount (could be also purchased OTC at a small discount) which are redeemable across a network of participating companies (although focusing on the travel and leisure sector); see https://bit.ly/2Hz4jjM. It has to be noted, however, there are differences between the scrips used in, e.g. lumber camps in the United States or the sugar cane mills in northern Argentina, and those issued by local (or even provincial) authorities, in that the creation of scrip currency and the provision of services (particularly those settled through the payment of taxes/service charges) were potentially done by different institutions.

[174] Worth recalling the word general has its root in the latin *generalis*, meaning "common to a whole class or kind" (as in *appellatio uasorum est generalis*, or "comprising a general appeal"; see *Corpus Iuris Civilis* 1598, p. 1430).

[175] Data to April 2, 2018. See https://bit.ly/2r9JMLp. Although widely adopted, the use of this concept in this context is somewhat contested unless considering virtual tokens to be securities, in which case they are not money (even if money is thought of a form of "debt security" in theory, it lacks all of the properties of debt securities in practice).

at the "thin end" of propagation.[176] Quite obviously, lacking any sanctioning by an authority the process greatly depends on the relationship among those people adopting it.[177] Despite their appeal, primarily because the available alternatives might impose operational or other constraints[178] many more actors and activity sectors need "opening up" to accepting these virtual tokens.

The appeal of censorship-resistant protocols, however, faces a practical hurdle: those blockchains can only enforce transactions taking place "inside" their ecosystem; therefore, a "trusted" third party is needed to provide the "infrastructure bridge" necessary to make the connection to the outside world, arguably defeating the very objective of ensuring censorship resistance.[XXXII] At the moment, this is a hurdle every virtual token has to overcome if aspiring to become a widely adopted medium of exchange. It also waters-down the debate (quite loud and abrasive at times) around the pros and cons of permissioned and permissionless protocols.

In any case, those are implementational issues that might just require technology (and a dose of patience) for a solution to be found; however, they do not tackle head-on the key question of desirability, on efficiency grounds, of a competitive supply of private notes in an economy that has a government-issued currency.[179] The answer to this question is far from being settled. The bulk of research on the

[176] In terms of how far, fast and deep its usage spreads.

[177] That depends on the shared interests or goals, hence if a virtual currency, say, "encapsulates" certain contextual meaning (as shown throughout the introduction and compementary information in Notes I to XII) then specific network structures would emerge between people who become "associated" to that virtual currency.

Besides the toy examples provided above, a clear, practical example can be found in the so-called utility tokens. Those tokens, either by design or by virtue of network effects, provide a means to perform or facilitate transactions as part of a closed ecosystem and could be defined as currency in a "narrow" sense.

Concerning the speed element (or how fast it could be adopted) it depends on the cohesiveness between users or homophily. Looking at it as a graph structure, this notion can be linked to how reachable are the nodes in each subgraph; subgraphs here denoting communities of users. The closer they are (or equivalently, the shorter the path length is between existing and potential users) the faster adoption becomes. This also suggests adoption is not necessarily dependent on the number of edges in those subgraphs.

In the examples provided above, such locally dense features emerge quite clearly (all the people in the town agree; all those trading a specific commodity or service agree). Note, in passing, that a group is deemed "local" if it is definable over subgraphs only induced by the group; therefore, it neglects the network existing outside of it.

[178] For example, wealth transferability or cross-border payments; in general, their advantage is frequently tied to particular situations and hence their use-value is quite subjective.

[179] The alternative is a model only having competing private suppliers of private money, along the postulates of the Free Banking School (in essence, a banking system without lender of last resort; see, e.g. Hayek 1978, White 1992, or Selgin 2008). This type of setup is used to explore if competition in the issuance of money is more efficient than a monopoly.

subject has focused on "tweaking" the model recently introduced by Lagos and Wright[180] that by now has become a workhorse of monetary theory.[181] The suggestion is that a "coexistence" regime between fiat money issued by the government and private currency leads to multiple equilibria, dominating each other in terms of welfare. The outcome depends on how "large" the private sector becomes relative to the government, up to a certain threshold.[182]

So far the behaviour of private entrepeneurs coming to the market as currency issuers has not been discussed, nor the potential consequences of using tokens whose price can change depending on future expectations. Furthermore, there is the question of social efficiency and the impact due to the pecuniary externalities[183] suggestive of a market for currencies that is not the same as the market for other goods and services, by any measure.

In other words, does currency competition guarantee the optimal quantity of money in an economy? The answer is not obvious.

8. Conclusion: virtual currencies and their future

The media of these tokens of wealth are, then,
in this process of exchange just such gestures
or symbols as language is in other fields.
G. H. Mead, 1934, p. 292

The 2007-2008 financial crisis has served as a reminder to society, if anything, of the political dimension of money. At the same time technological innovations have shown how ductile, both in its form and its interpretation,[184] money can become. Bitcoin is the poster child of a movement that seeks to re-politicise money away from institutions and

[180] See Lagos and Wright (2005).

[181] Once again, money becomes "essential" in the Lagos and Wright model (as in earlier models of money and search like, e.g. Kiyotaki and Wright 1993, Trejos and Wright 1995, or Shi 1995) because agents cannot monitor each other and hence gauge whether to accept or not money in an exchange.

[182] The intuition behind this result is that due to the different rates of return on private currency and fiat money, people begin to show preferences. So, in order to decide on the medium of exchange to accept in trade (or, let's say, its "colour") agents look at the obvious: how valuable the asset is, and how easy is to trade it in the future (acceptability by other agents). This gives raise to strategic complementarities leading to a range of Pareto-ranked steady state solutions. In decentralised markets using random matching technology, the outcome might not be the most preferred steady state unless the private histories of all agents become public.

[183] As in Wallace (2001).

[184] That is, both algorithmic malleability and the impact of technology-led platforms, such as Social Media, through which a narrative (or several, perhaps) about what those algorithmic solutions could "bring to the table" is insistently pushed.

the oversight by central banks.[185] The technology behind Bitcoin and other virtual "currencies" is inherently neutral but its implementation is not. In the introduction and elsewhere throughout this paper, factual evidence has shown Satoshi Nakamoto made a number of key design decisions following a (quite vocal at times) political blueprint; in that sense, it cannot be claimed that Bitcoin features, such as decentralisation, artificially generated scarcity and deflationism were anything but deliberate (as were the decisions, e.g. by cypherpunks many years before). In addition, the developments in search and matching models of money since the 1993 seminal paper by Kiyotaki and Wright have brought the promise of a microfoundations-based theory of money. On the one hand, they look at monetary transactions as decentralised, bilateral and time consuming exchanges; on the other hand, they rationalise how frictions in the exchange process lead to money's essentiality, unless, of course, functional alternatives to money are not feasible or do not yield better allocations than what is achievable using money.

Be that as it may, although all of the above efforts make a serious attempt to understand the logic of a monetary economy (building a rich, varied and ever growing literature) none completely succeeds at explaining why there is money in the first place, or even why money has a positive value. From a technical standpoint, either money is plugged into an otherwise standard Arrow-Debreu economy, or if essential in a decentralised economy its technology is simply imposed by design rather than becoming endogenous to the economy it helps to explain.[186]

Fortunately there are some clues (contestable, but clues nevertheless) to answer the question of why there is money. As discussed in the previous pages, money provides a distinctive, real service directly derived from the social contract.[187] That very fact explains, and

[185] It could be argued the origins of virtual money, not just bitcoin, can be traced back to a community where many believed that money itself could be used to challenge the *status quo*.

[186] Such monetary exchange technology is implicitly assumed to be "accepted" by economic agents. Everyone plays by the rules, or is otherwise excluded. As a matter of fact, there is no big difference between the "game designer" imposing such technology in search-theoretic models and the Walrasian "imaginary" auctioneer that sets prices (economics "unmoved mover").

[187] That social contract, either explicitly of tacitly agreed, is the link between citizens and the State (as outlined in Hobbes, Rousseau or Locke). But what should be understood as State? Although Weber in his *Wirtschaft und Gesellschaft* defined the State as "one of the forms of government," perhaps Hans Kelsen made things clearer when saying

> The state is, so to speak, a common point into which various human actions are projected... To impute a human action to the state, as to an invisible person, is to relate a human action as the action of a state organ to the unity of the order which stipulates this action. The state as a person is nothing but the personification of this unit. See Kelsen (1949, p. 191).

In that sense, the State becomes a "legal person" that is separate from society and from the government, but because a legal person does not exist as such (only as

much of the factual evidence seems to confirm, why there is a clear distinction between money and currency: money is always a currency, but currencies are not always money.

So where does that leave those new, virtual tokens such as bitcoin?

> `Proposition 1` – Virtual tokens are not money unless sanctioned by a government even if, someday, they become a unit of account owing to being the asset having the highest subjective probability of trade.[188]

Can they be simply considered as a new form of currency? That would require those virtual tokens to become widely accepted as medium of exchange. Recall the question of acceptance was discussed in Section 7 and elsewhere in this paper.

> `Proposition 2a` – Considering all of the virtual tokens nowadays in circulation or to be launched in the future, only those defined as utility tokens could be deemed to be a currency[189] but only in a "narrow sense."[190]
>
> `Proposition 2b` – Virtual tokens that are not construed as utility tokens[191] could, in principle, become a medium of exchange, unit of account and ultimately a store of value if individuals perceive them as stable.

---

a concept) it can only operate through members of the community. That is how a government emerges.

The social "contract" rests, hence, on a bilateral governance compact where Citizens freely delegate certain roles and responsibilities to the government which, in exchange, provides collective goods (e.g. the rule of law, protection of property rights, security).

[188] See Section 3. The ability of an instrument to discharge obligations with the government (acceptance as means of payment for immediate settlement, on request, of fiscal debts) transforms that instrument into money.

[189] The definition of a utility token adopted here reflects, to some extent, that of FINMA (the Swiss Financial Market Supervisory Authority) in its 2018 ICO Guidelines, published on February 16, 2018. According to FINMA (in section 3.1 of the aforementioned guidelines) utility tokens are those "which are intended to provide access digitally to an application or service by means of a blockchain-based infrastructure." Here, this definition is extended to tokens that also serve a means of payment (settlement) for transactions conducted within the ecosystem defined by said "application or service." Upon the platform becoming operational, those tokens attain a strictly positive value and hence could be deemed a currency. See also footnote 177.

We're excluding yet another class of tokens, the so-called "security" tokens, which are digital representations of financial securities (e.g. equity or bonds).

[190] Narrow here means that a token becomes a currency within the ecosystem for which they were created. This constraint does not preclude competition from other entrepeneurs in any given vertical.

[191] The distinction applies because the utility tokens have a "functional" component in them related to the service they provide in their ecosystem. Stability, in this case, predominantly impacts their ability to trade in a secondary market; the assumption made here is that such tokens become *de facto* units of account at least within their respective ecosystems (so settlement of obligations always, or primarily, takes place using those tokens).

There is, of course, the question of what is meant by "stable" and the conditions to achieve such stability. Proposition `2b` seems rather obvious, but agent's expectations about the future (not necessarily linked to the mechanics that provide stability to the token) can change the valuation of a token to zero; in other words, there is a set of equilibrium trajectories that include zero as possible outcome. Why? Each agent willing to receive a private token forms a belief as to the future exchange value of that token. There will be *de facto* multiple beliefs, depending on the individual agents' "decision windows" (discussed in Section 5) and their views as to the reputation of the token issuer (note, however, both features are not necessarily linked). Thus, multiple beliefs will exist that are consistent with an equilibrium outcome, one being zero.

In addition, the following condition is proposed (for the time being) without proof.

> `Proposition 3` – Stability could only be attained if the minting technology is weakly convex.[192]

The next issue relates to the possibility of privately-issued tokens ever becoming adopted as currency in an environment where they will certainly compete with government-issued money (a hybrid system).[193] We state the following as a proposition, again without proof, a task left for this paper's sequel.

> `Proposition 4` – Currency competition can only succeed if the issuance of private tokens is bounded.[194]

In other words, players have to adhere to monetary discipline.[195] In this context, it means the suppliers of private currency, for a given production technology, do not pursue profit maximisation. This blends with the idea of decoupling the supply of virtual tokens (currency supply) from the maintenance of the transaction ledger.

[192] This excludes, e.g. POW-based coin generation technologies as implemented in Bitcoin and similar platforms. It therefore seems that bitcoin and similar coins will carry on as (yet another) asset class but will unlikely ever become a currency.

[193] Or equivalently, an economy where the government does not print money but regulates private issuance so to match its policy objectives.

[194] It could be argued here that bitcoin satisfies this criteria by design.

[195] Although this proposition seems obvious at first sight it is not, considering that those private suppliers of currency might pursue profit maximisation as sole objective. It is linked to `Proposition 3` concerning the production technology.

The previous discussion reflects the general idea and message of this paper. People discuss cryptocurrencies, but usage of the "currency" qualifier is almost invariably misplaced. Back in the day it was an ideology-toned marketing gig, nothing else. The only exceptions are, possibly, the few tokens backing clear use cases (utility tokens) which, once their application ecosystem matures, will behave as currencies within those domains.[196]

For now, it would be more accurate to speak about virtual tokens that are like money; or "moneyness," perhaps in the sense of it depicting "a relational property that concerns the potential and the power of becoming and being like money the social fact, and process rather than the quantitative expression."[197] So those virtual tokens are not quite the thing one calls money, but "the realisation of money, the process"[198] which is defined by what people believe money should be, or has become.

Does that mean that "cryptos" (to be more precise) cannot become currencies in a broader defintion of the term? Of course not. That said, to be (or, again to be precise, aspire becoming) a widely accepted medium of exchange, cryptos need to be conceptually redesigned. That is the subject of `Part 2` of this White Paper.

[196] In many ways resembling the virtual currencies that have been used in the synthetic economies of online gaming since the late 90's; e.g. World of Warcraft (WoW). An interesting feature of WoW is that the platform has several "realms" or stand-alone economies, and that transactions are nearly impossible between them. That said, it seems there was actually a thriving and at times quite workable services sector online that specialised in transfers between realms (thanks to Nicolas Jacquemart for pointing this out).

[197] See Zickgraf (2017, p. 306).

[198] Ibid., p. 321.

References

Oxford Latin Dictionary. Oxford, UK: Oxford University Press, 1968.

G. Akerlof. The market for "lemons": Quality uncertainty and the market mechanism. Quarterly Journal of Economics, 84(3):488–500, 1970.

C. G. Aliprantis, C. D. and D. Puzzello. A random matching theory. Krannert working paper #1168, Purdue University, 2004.

A. Appadurai. Banking on Words: The Failure of Language in the Age of Derivative Finance. Chicago and London: University of Chicago Press, 2016.

P. Arestis. The Post-Keynesian Approach to Economics: An Alternative Analysis of Economic Theory and Policy. London: Edward Elgar Publishing, 1992.

P. Arestis and A. S. Eichner. The post-keynesian and institutionalist theory of money and credit. Journal of Economic Issues, 22(4):1003–1021, 1988.

Aristotle. The Nicomachean Ethics. Oxford World's Classics. Oxford, UK: Oxford University Press, 2004.

K. J. Arrow and G. Debreu. Existence of equilibrium for a competitive economy. Econometrica, 22(3):265–290, 1954.

S. Ball Platner and T. Ashby. A Topographical Dictionary of Ancient Rome. London: Humphrey Milford. Oxford University Press, 1929.

A. V. Banerjee and E. S. Maskin. A walrasian theory of money and barter. Quarterly Journal of Economics, 111(4):955–1005, 1996.

P. Bayle. The dictionary historical and critical of Mr. Peter Bayle. London: Thoemmes Press, 1736.

A. Berentsen. On the private provision of fiat currency. European Economic Review, 50(7):1683–1698, 2006.

A. Berentsen, G. Camera, and C. Waller. The distribution of money balances and the non-neutrality of money. International Economic Review, 46(2):465–487, 2005.

A. Berentsen, S. Huber, and A. Marchesiani. Limited commitment and the demand for money. ECON working paper 199, Department of Economics, University of Zurich, February 2016.

A. Berentsen, M. Molico, and R. Wright. Indivisibilities, lotteries, and monetary exchange. Journal of Economic Theory, 107(1):70–94, 2002.

A. Berentsen and F. Schar. A short introduction to the world of cryptocurrencies. Federal Reserve Bank of St. Louis Review, 100(1):1–16, 2018.

A. Berentsen and C. Waller. Price level targeting and stabilization policy. Journal of Money, Credit and Banking, 43(2):559–580, 2011.

G. Berkeley. The Querist. Edited by A. A. Luce and T. E. Jessop. Edinburgh, UK: Thomas Nelson & Sons, 1953.

V. Bignon. Cigarette money and black market prices around the 1948 german miracle. Working paper 2009-02, Universite de Paris Ouest Nanterre La Defense, January 2009.

E. Bleiberg. The Official Gift in Egypt. Norman, OK: University of Oklahoma Press, 1996.

E. Bleiberg. Loans, credit and interest in ancient egypt. In M. Hudson and M. D. Mieroop, editors, Debt and Economic Renewal in the Ancient Near East, pages 257–276. Bethesda, MD: CDL Press, 2002.

P. Bohannan. The impact of money on an african subsistence economy. Journal of Economic History, 198(4):491–503, 1959.

J. Bonar. Knapp's theory of money. The Economic Journal, 32(125):39–47, 1922.

P. Bourdieu. Algeria 1960: The Disenchantment of the World; The Sense of Honour; The Kabyle House, or, the World Reversed. Cambridge, UK: Cambridge University Press, 1979.

K. Brunner. Money supply. In M. M. J. Eatwell and P. Newman, editors, The New Palgrave: Money, pages 263–267. New York and London: W. W. Norton & Company, 1989.

J. M. Buchanan and G. F. Thirlby. L.S.E. Essays on Cost. New York: New York University Press, 1981.

C. G. Caffentzis. Exciting the Industry of Mankind: George Berkeley's Philosophy of Money. Number 170 in International Archives of the History of Ideas. Dordrecht: Springer Science+Business Media, 2000.

R. Calvacanti and N. Wallace. Inside and outside money as alternative media of exchange. Journal of Money, Credit and Banking, 31(3):443–457, 1999. Part 2: The Role of Central Banks in Money and Payments Systems.

J. G. Carrier, ed. A Handbook of Economic Anthropology. Cheltenham: Edward Elgar, 2005.

B. G. Carruthers and S. Babb. The color of money and the nature of value: Greenbacks and gold in postbellum america. American Journal of Sociology, 101(6):1556–1591, 1996.

B. G. Carruthers and S. Babb. The color of money and the nature of value: Greenbacks and gold in postbellum america. American Journal of Sociology, 101(6):1556–1591, 1996.

D. Cass and K. Shell. In defense of a basic approach. In J. H. Kareken and N. Wallace, editors, Models of Monetary Economies, pages 251–260. Minneapolis: Federal Reserve Bank of Minneapolis, 1980.

E. Castronova. Wildcat Currency: How the Virtual Money Revolution is Transforming the Economy. New Haven & London: Yale University Press, 2014.

V. Chappell, ed. The Cambridge Companion to Locke. Cambridge, UK: Cambridge University Press, 1994.

A. Christoyannopoulos, ed. Religious Anarchism: New Perspectives. Newcastle: Cambridge Scholars Publishing, 2009.

M. T. Cicero. The Orations of Marcus Tullius Cicero. Trans. by C. D. Yonge; Covent Garden: H. G. Bohn, 1856.

M. T. Cicero. Letters to Atticus. Trans. by E. O. Winstedt; London: W. Heinemann, 1913.

M. T. Cicero. On Old Age. On Friendship. On Divination. Loeb Classical Library 154. Trans. by W. Flaconer; Boston, MA: Harvard University Press, 1923.

R. W. Clower. A reconsideration of the microfoundations of monetary theory. Western Economic Journal (now Economic Inquiry), 6(1):1–8, 1967.

A. J. Cohen, H. Hagemann, and J. Smithin. Money, Financial Institutions and Macroeconomics. New York: Springer Science+Business Media, 1997.

R. W. Cooper, D. V. DeJong, R. Forsythe, and T. W. Ross. Selection criteria in coordination games: some experimental results. American Economic Review, 80(1):218–233, 1990.

R. W. Cooper, D. V. DeJong, R. Forsythe, and T. W. Ross. Communication in coordination games. Quarterly Journal of Economics, 107(2):739–771, 1992.

R. W. Cooper, D. V. DeJong, R. Forsythe, and T. W. Ross. Forward induction in coordination games. Economics Letters, 40(2):167–172, 1992.

G. Dalton. Primitive money. American Anthropologist (New Series), 67(1):44–65, 1965.

P. Davidson. Money and the real world. The Economic Journal, 82(325):101–115, 1972.

J. Davies, R. Lluberas, and A. Shorrocks. Global wealth report 2017: Where are we ten years after the crisis? Technical report, Credit Suisse Research Institute, 2017.

M. de Cecco and J. Fitoussi. Monetary Theory and Economic Institutions. Proceedings of a Conference held by the International Economic Association. New York: Palgrave Macmillan, 1987.

M. de Cecco and J. Fitoussi. Monetary Theory and Economic Institutions. Edited by M. von Mises and R. M. Ebeling. Dordrecht: Springer, 1990.

P. Diamond. Money in search equilibrium. Econometrica, 52(1):1–20, 1984.

D. Dillard. Keynes and marx: A centennial appraisal. Journal of Post Keynesian Economics, 6(3):421–432, 1984.

D. Dillard. Money as an institution of capitalism. Journal of Economic Issues, 21(4):1623–1647, 1987.

V. R. Dominguez. Representing value and the value of representation: A different look at money. Cultural Anthropology, 5(1):16–44, 1990.

J. Duffy and J. Ochs. Emergence of money as a medium of exchange: An experimental study. American Economic Review, 89(4):849–877, 1999.

J. Duffy and J. Ochs. Intrinsically worthless objects as media of exchange: Experimental evidence. International Economic Review, 43(3):637–673, 2002.

J. Duffy and D. Puzzello. Gift exchange versus monetary exchange: Theory and evidence. American Economic Review, 104(6):1735–1776, 2014.

S. Durlauf and L. E. Blume. The New Palgrave: Monetary Economics. Basingstoke, UK: Palgrave Macmillan, 2010.

J. Ehremberg. Civil Society: The Critical History of an Idea. New York and London: New York UNiversity Press, 1999.

P. Einzig. Primitive Money. Oxford, UK: Pergamon Press, 1966.

A. M. Endres. Neoclassicam Microeconomic Theory: The Founding Austrian Version. London and New York: Routledge, 2002.

N. Ferguson. The Ascent of Money: A Financial History of the World. New York: The Penguin Press, 2008.

I. Fisher. The Purchasing Power of Money: Its Determination and Relation to Credit, Interest and Crises. New York: The Macmillan Company, 1920.

L. C. Freeman. The Development of Social Network Analysis: A Study in the Sociology of Science. Vancouver, BC: Empirical Press, 2004.

M. Friedman. Commodity-reserve currency. Journal of Political Economy, 59(3):203–232, 1951.

M. Friedman. Commodity-Reserve Currency. Journal of Political Economy, 5(3):203–232, 1951.

M. Friedman and A. Schwartz. A Monetary History of the United States, 1867-1960. National Bureau of Economic Research Publications. Princeton, NJ: Princeton University Press, 1963.

D. Gale. Money: In Equilibrium. Cambrdige, UK: Cambridge University Press, 1982.

D. Godefroy. Corpus Iuris Civilis, volume 2. Guillelmus Laemarius, 1598.

M. Godelier. Perspectives in Marxist Anthropology. Cambridge Studies in Social Anthropology. Cambridge, UK: Cambridge University Press, 1977.

M. Godelier. The Enigma of the Gift. Chicago: University of Chicago Press, 1999.

G. M. Gomez. Argentina's Parallel Currency: The Economy of the Poor. Financial History Series. London: Pickering & Chatto, 2009.

G. M. Gomez. Varieties of money and currency circuits in argentina (2000-2002). Sciences Po, Lyon, France, June 2016. Monetary institutionalisms in the French Speaking world.

C. A. E. Goodhart. The two concepts of money: implications for the analysis of optimal currency areas. European Journal of Political Economy, 14(3):407–432, 1998.

D. Goodway. Anarchist Seeds beneath the Snow: Left-Libertarian Thought and British Writers from William Morris to Colin Ward. Liverpool: Liverpool University Press, 2006.

A. W. Gouldner. The norm of reciprocity: A preliminary statement. American Sociological Review, 25(2):161–178, 1960.

D. Graever. Toward An Anthropological Theory of Value: The Flse Coin of our Dreams. New York: Palgrave, 2001.

J. Grandmont. Money and Value: A Reconsideration of Classical and Neoclassical Monetary Theories. Econometric Society Monographs in Pure Theory. Cambridge, UK: Cambridge University Press, 1999.

C. A. Gregory. Gifts and Commodities. London: Academic Press, 1982.

P. Grierson. The origins of money. Research in Economic Anthropology, 1:1–35, 1978.

J. G. Gurley and E. S. Shaw. Money in a Theory of Finance. Washington, DC: The Brookings Institution, 1960.

F. H. Hahn. On some problems of proving the existence of an equilibrium in a monetary economy. In F. H. Hahn and F. Brechling, editors, The Theory of Interest Rates, pages 126–135. London: Macmillan, 1965.

F. H. Hahn. Equilibrium with transaction costs. Econometrica, 39(3):417–439, 1971.

F. H. Hahn. On the notion of equilibrium in economics. Inaugural lecture, University of Cambridge, 1973.

F. H. Hahn. On transaction costs, inessential sequence economies and money. The Review of Economic Studies, 40(4):449–461, 1973.

F. H. Hahn. Money and Inflation. Cambridge, MA: The MIT Press, 1983.

F. H. Hahn. Aspects of Monetary Theory. Number 368 in Rheinisch-Westfalische Akademie der Wissenschaften. Dusseldorf: Westdeutscher Verlag, 1989.

H. Halaburda and M. Sarvary. Beyond Bitcoin: The Economics of Digital Currencies. London: Palgrave Macmillan, 2016.

A. Hamilton. The Federalist: A Collection of Essays Written in Favour of the New Constitution. New York: J. and A. Mc. Lean, 1878.

W. H. Hamilton. The institutional approach to economic theory. American Economic Review, 9(1):309–318, 1919.

X. Han, P. Kelsen, V. Ramachandran, and R. E. Tarjan. Computing minimal spanning subgraphs in linear time. SIAM Journal of Computing, 24(6):1332–1358, 1995.

R. Harrod. Money. London: Macmillan and Co., 1969.

K. Hart. The Memory Bank: Money in an Unequal World. London: Profile Books, 2000.

F. Haslinger. Money and barter in general equilibrium: A review. Journal of Economics, 39(3-4):385–400, 1979.

F. Hayek. The Denationalisation of Money–The Argument Refined. London: Institute of Economic Affairs, 1978.

D. He and IMF Staff Team. Virtual currencies and beyond: Initial considerations. Staff discussion notes, International Monetary Fund - SDN/16/03, January 2016.

E. Helleiner. National currencies and national identities. American Behavioral Scientist, 41(10):1409–1436, 1998.

M. F. Hendy. Studies in the Byzantine Monetary Economy C.300-1450. Cambridge, UK: Cambridge University Press, 2008.

J. F. Henry. The social origins of money: The case of egypt. Mimeo, California State University, Sacramento, 2002.

J. Hicks. Value and Capital: An Inquiry into some Fundamental Principles of Economic Theory. London: Oxford University Press, 1939.

J. Hicks. Critical Essays in Monetary Theory. Oxford, UK: Clarendon Press, 1967.

J. R. Hicks. A Market Theory of Money. Oxford, UK: Oxford University Press, 1989.

J. Hirshleifer. The private and social value of information and the reward to inventive activity. American Economic Review, 61(4):561–574, 1971.

T. Hobbes. Leviathan or the Matter, Forme, & Power of a Common-Wealth Ecclesiasticall and Civill. London: Andrew Crooke, 1651.

G. M. Hogdson. What are institutions? Journal of Economic Issues, 40(1):1–25, 2006.

J. Hogendorn and M. Johnson. The Shell Money of the Slave Trade. Cambridge, UK: Cambridge University Press, 1986.

J. Huber. Sovereign Money: Beyond Reserve Banking. Cham: Palgrave Macmillan, 2017.

C. Humphrey. Fair dealing, just rewards: the ethics of barter in north-east nepal. In C. Humphrey and S. Hugh-Jones, editors, Barter, Exchange and Value: An Anthropological Approach, pages 107–141. Cambridge, UK: Cambridge University Press, 1992.

S. E. Hutchinson. Nuer Dilemmas: Coping with Money, War, and the State. Berkeley: University of California Press, 1996.

G. Ingham. Money is a social relation. Review of Social Economy, 54(4):507–529, 1996.

G. Ingham. The nature of money. Cambridge, UK and Malden, MA: Polity Press, 2004.

A. M. Innes. What is money? The Banking Law Journal, 30:377–408, 1913.

A. M. Innes. The credit theory of money. The Banking Law Journal, 31:151–168, 1914.

K. Iwai. Evolution of money. In A. Nicita and U. Pagano, editors, The Evolution of Economic Diversity, pages 396–431. London and New York: Routledge, 2013.
W. Jaffe. Menger, Jevons and Walras de-homogenized. Economic Inquiry, 14(4):511–524, 1976.
W. S. Jevons. The Theory of Political Economy. London and New York: Macmillan and Co., 1871.
W. S. Jevons. Money and the Mechanism of Exchange. New York and London: D. Appleton and Company, 1919 (1875).
S. Kaviraj and S. Khilnani. Civil Society: History and Possibilities. Cambridge, UK: Cambridge University Press, 2001.
L. A. Keister. Financial markets, money, and banking. Annual Review of Sociology, 28:39–61, 2002.
K. Kelly. Out of Control: The New Biology of Machines, Social Systems and the Economic World. Author's Edition, 1994.
P. H. Kelly. John Locke: Locke on Money - Vol 1 and 2. Oxford, UK: Clarendon Press, 1991.
H. Kelsen. General Theory of Law and State. The 20th Century Legal Philosophy Series. London: Oxford University Press, 1949.
B. J. Kemp. Ancient Egypt: Anatomy of a Civilization. Abingdon, UK: Routledge, 2006.
J. M. Keynes. What is money? Review article in Economic Journal, 24(95):419–421, 1914.
J. M. Keynes. The General Theory of Employment, Interest and Money. New York: Harcourt Brace Jovanovich, 1964.
H. S. Kim. Small change and the moneyed economy. In E. E. C. P. Cartledge and L. Foxhall, editors, Money, Labour and Land: Approaches to the Economies of Ancient Greece, pages 44–53. London and New York: Routledge, 2002.
A. P. Kirman. Whom or what does the representative individual represent? Journal of Economic Perspectives, 6(2):117–136, 1992.
N. Kiyotaki and R. Wright. A search-theoretic approach to monetary economics. American Economic Review, 83(1):63–77, 1984.
B. Klein. The competitive supply of money. Journal of Money, Credit and Banking, 6(4):423–453, 1974.
D. Klose. Solidus. In H. Cancik and H. Schneider, editors, Der Neue Pauly, volume 11. Stuttgart: Metzler, 2001.
G. F. Knapp. The State Theory of Money. London: Macmillan & Company, 1924.
F. H. Knight. The common sense of political economy (wicksteed reprinted). Journal of Political Economy, 42(5):660–673, 1934.
N. Kocherlakota. Money is memory. Journal of Economic Theory, 81(2):232–251, 1998.
N. Kocherlakota. Money: What's the question and why should we care about the answer? American Economic Review, 92(2):58–61, 2002.
R. E. Kranton. Reciprocal exchange: A self-sustaining system. American Economic Review, 86(4):830–851, 1996.
J. Kroll. Observation of monetary instruments in pre-coinage greece. In M. S. Balmuth, editor, Hacksilber to Coinage: New Insights into the Monetary History of the Near East and Greece, pages 77–916. New York: American Numismatic Society, 2001.

J. Kroll. The monetary background of early coinage. In W. E. Metcalf, editor, The Oxford Handbook of Greek and Roman Coinage, pages 33–42. Oxford, UK: Oxford University Press, 2012.

L. Kurke. Coins, Bodies, Games, and Gold: The Politics of Meaning in Archaic Greece. Princeton, NJ: Princeton University Press, 1999.

P. Lacoste. La crisis socioeconomica argentina y las respuestas sociales: las redes de clubes de trueque. Revista Confluencia, 1(1), 2003.

R. Lagos and R. Wright. A unified framework for monetary theory and policy analysis. Journal of Political Economy, 113(3):463–484, 2005.

D. Laidler. Notes on the microfoundations of monetary economics. The Economic Journal, 107(443):1213–1223, 1997.

D. Laidler and N. Rowe. George simmel's philosophy of money: A review article for economists. Journal of Economic Literature, 18(1):97–105, 1980.

M. Lamont. Toward a comparative sociology of valuation and evaluation. Annual Review of Sociology, 38(1):201–221, 2012.

L. H. Lapham. Money and class in America: Notes and Observations on Our Civil Religion. London: Weidenfeld & Nicolson, 1988.

J. L. Laughlin. The principles of money. New York: C. Scribner's Sons, 1903.

M. Lavoie. Post-Keynesian Economics: New Foundations. London: Edward Elgar Publishing, 2014.

A. P. Lerner. Money as a creature of the state. The American Economic Review, 37(2):312–317, 1947.

E. Lindhal. Studies in the Theory of Money and Capital. New-York: Augustus M. Kelley, 1939.

E. Lo Cascio. State and coinage in the late republic and early empire. Journal of Roman Studies, 71:76–86, 1981.

C. Lorber. The coinage of the ptolemies. In W. Metcalf, editor, The Oxford Handbook of Greek and Roman Coinage, pages 211–234. Oxford, UK: Oxford University Press, 2012.

R. E. Lucas, Jr. Equilibrium in a pure currency economy. Economic Inquiry, 18(2):203–20, 1980.

N. Machiavelli. The Prince. New York: Penguin Books, 1961. Translation by G. Bull.

B. Malinowski. Argonauts of the Western Pacific: An Account of Native Enterprise and Adventure in the Archipelagoes of Melanesian New Quinea. London: Routledge, 2002.

J. G. Manning. Coinage as 'code' in ptolemaic egypt. Princeton/stanford working papers in classics, Stanford University, December 2006.

J. R. V. Marchant and J. F. Charles. Cassell's Latin Dictionary. New York: Funk & Wagnalls Company, 1953.

G. E. Markoe. Phoenicians. Berkeley, CA: University of California Press, 2000.

A. Marsh. Money and Modernity: Pound, Williams, and the Spirit of Jefferson. Tuscaloosa: The University of Alabama Press, 1998.

A. Marshall. Principles of Economics. Plagrave Classics in Economics. Basingstoke, UK: Palgrave Macmillan, 2013.

B. Maurer. The anthropology of money. Annual Review of Anthropology, 35:15–36, 2006.

G. Mauss. The Gift: The Form and Reason for Exchange in Archaic Societies. Routledge Classics. London and New York: Routledge, 2002.

K. A. McCabe. Fiat money as a store of value in an experimental market. Journal of Economic Behavior and Organization, 12(2):215–231, 1989.

H. D. Mcleod. The Theory and Practice of Banking, Vol. 2. London: Longmans, Green, Reader & Dyer, 1866.

H. D. Mcleod. Lectures on Credit and Banking. London: Longmans, Green and Company, 1882.

H. D. Mcleod. The Theory of Credit. London: Longmans, Green and Company, 1889.

G. H. Mead. Mind, Self and Society from the Standpoint of a Social Behaviorist. Chicago, IL: The University of Chicago Press, 1934. Edited by W. C. Morris.

C. Menger. On the origin of money. The Economic Journal, 2(6):239–255, 1892.

C. Menger. Principles of Economics. New York: New York University Press, 1981 (1871).

D. Miano. Moneta: Sacred memory in mid-republican rome. In M. Bommas, J. Harrisson, P. Roy, and E. Theodorakopolous, editors, Memory and Urban Religion in the Ancient World, pages 89–106. London: Bloomsbury, 2012.

H. P. Minsky. Stabilizing an Unstable Economy. New York: McGraw Hill, 2008.

W. C. Mitchell. The limitations of marginal utility. Journal of Political Economy, 17(9):620–636, 1909.

W. C. Mitchell. The role of money in economic theory. American Economic Review, 6(1):140–161, 1916.

W. C. Mitchell. The prospects of economics. In R. G. Tugwell, editor, The Trend of Economics, pages 3–34. New York: Alfred A. Knopf, 1924.

C. Monnet. Private versus public money. International Economic Review, 47(3):951–960, 2006.

J. Niehans. Money and barter in general equilibrium with transaction costs. American Economic Review, 61(1):773–783, 1971.

E. Nosal and G. Rocheteau. Money, Payments, and Liquidity. Cambridge, MA: The MIT Press, 2011.

J. M. Ostroy. The informational effciency of monetary exchange. American Economic Review, 63(4):597–610, 1973.

J. M. Ostroy and R. M. Starr. The transactions role of money. In B. M. Friedman and F. H. Hahn, editors, Handbook of Monetary Economics, volume 1, pages 3–62. Amsterdam: North-Holland, 1990.

J. Parry and e. M. Bloch. Money and the Morality of Exchange. Cambridge, UK: Cambridge University Press, 1996.

D. Patinkin. Money, Interest, and Prices: An Integration of Monetary and Value Theory. New York: Harper and Row, 1965.

D. W. Pearce. The MIT Dictionary of Modern Economics. London: The MIT Press, 1992.

D. Pedersen. The storm we call dollars: Determining value and belief in el salvador and the united states. Cultural Anthropology, 17(3):431–459, 2002.

N. Piffaretti. A theoretical approach to electronic money. Mimeo, Faculte de Sciences Economiques et Techniques - University of Fribourg, 1998.

C. D. Piot. Of persons and things: Some reflections on african spheres of exchange. Man (New Series), 26(3):405–424, 1991.

K. Polanyi. The Great Transformation: The Political and Economic Origins of our Time. New York: Farrar & Rinehart, 1944.
N. Popper. Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money. San Francisco: Harper Collins, 2015.
A. H. Quiggin. A Survey of Primitive Money: The Beginnings of Currency. London: Meuthen and Co., 1949.
R. Radner. Competitive equilibrium under uncertainty. Econometrica, 36(1):31–58, 1968.
R. Radner. Existence of equilibrium of plans, prices, and price expectations in a sequence of markets. Econometrica, 40(2):289–303, 1972.
G. Ritter. Goldbugs and Greenbacks: The Antimonopoly Tradition and the Politics of Finance in America. Cambridge, UK: Cambridge University Press, 1997.
L. Rochon and M. Vernego. Money and the real world: Or chartalism and its discontents. Journal of Post Keynesian Economics, 26(1):57–67, 2003.
M. M. Rothbard. The austrian theory of money. In E. G. Dolan, editor, The Foundations of Modern Austrian Economics, pages 160–184. Kansas City, KA: Sheed & Ward, 1976.
D. Rowe. The Real Meaning of Money. San Francisco: Harper Collins, 1997.
D. Rutherford. Routledge Dictionary of Economics. London and New York: Routledge, 2002.
H. Sabourian and L. Anderlini. Some notes on the economics of barter, money and credit. In C. Humphrey and S. Hugh-Jones, editors, Barter, Exchange and Value: An Anthropological Approach, pages 75–106. Cambridge, UK: Cambridge University Press, 1992.
M. D. Sahlins. Stone Age Economics. Chicago and New York: Aldine-Atherton, 1972.
J. A. Schumpeter. History of Economic Analysis. London: Routledge, 1986.
B. Schwartz. The social psychology of the gift. In A. E. Komter, editor, The gift: An Interdisciplinary Perspective, pages 69–80. Amsterdam: Amsterdam University Press, 1996.
J. R. Searle. The Construction of Social Reality. New York: Simon & Shuster, 1995.
J. R. Searle. What is an institution? Journal of Institutional Economics, 1(1):1–22, 2005.
G. A. Selgin. Good Money: Birmingham Button Makers, the Royal Mint and the Beginnings of Modern Coinage, 1775-1821. Ann Arbor: University of Michigan Press, 2008.
G. A. Selgin. Quasi-commodity money. Mimeo, University of Georgia Department of Economics, January 2012.
S. Shi. Money and prices: A model of search and bargaining. Journal of Economic Theory, 67(2):467–496, 1995.
S. Shi. A divisible search model of fiat money. Econometrica, 65(1):75–102, 1997.
S. Shi. Viewpoint: A microfoundation of monetary economics. Canadian Journal of Economics, 39(3):643–688, 2006.
M. Shubik. The Theory of Money and Financial Institutions, volume 1-2. Cambridge, MA: The MIT Press, 1999.
P. Sillitoe. Why spheres of exchange? Ethnology, 45(1):1–23, 2006.
G. Simmel. The Philosophy of Money. London and New York: Routledge, 2004.

A. Smith. An Inquiry into the Nature and Causes of The Wealth of Nations. Edinburgh: Adam and Charles Black, 1859.

T. Smith. Currency and Banking: Being an Attempt to Show their True Nature, and to Explain the Difficulties that have Occurred in Discussing them. Philadelphia, PA: Jesper Harding, Printer, 1832.

A. Sohn-Rethel. Intellectual and Manual Labor: A Critique of Epistemology. Atlantic Highlands, NJ: Humanities Press, 1978.

R. Solomon. Money on the move: The revolution in international finance since 1980. Princeton, NJ: Princeton University Press, 1999.

D. Sperber. Roman Palestine, 200-400: Money and prices. Bar-Ilan studies in Near Eastern languages and culture. Ramat Gan: Bar-Ilan University Press, 1991.

R. M. Starr. General Equilibrium Models of Monetary Economies: Studies in the Static Foundations of Monetary Theory. San Diego: Academic Press, 1989.

R. M. Starr. The jevons double coincidence condition and local uniqueness of money: An example. Journal of Mathematical Economics, 46(5):786–792, 2010.

R. M. Starr. Why is There Money? Walrasian General Equilibrium Foundations of Monetary Theory. Cheltenham: Edward Elgar, 2012.

R. M. Starr. Why Is There Money? Endogenous Monetization of an Arrow-Debreu Economy. The Rolf Mantel Lecture. Asociacion Argentina de Economia Politica, 2017.

M. Strathern. Qualified value: The perspective of gift exchange. In C. Humphrey and S. Hugh-Jones, editors, Barter, Exchange and Value: An Anthropological Approach, pages 169–191. Cambridge, UK: Cambridge University Press, 1992.

M. Strathern. Kinship, Law and the Unexpected: Relatives Are Always a Surprise. Cambridge, UK: Cambridge University Press, 2005.

W. Stukeley. The Medallic History of Marcvs Avrelivs Valerivs Caravsivs: Emperor in Brittain. London: Charles Corbet, 1757.

C. Tacitus. Germania. In R. Potter, editor, The Germania of Tacitus. Middletown, CT: American Philological Association, 1935.

J. B. Taylor. Aggregate dynamics and staggered contracts. Journal of Political Economy, 88(1):1–23, 1980.

H. Thornton. An Enquiry Into the Nature and Effects of the Paper Credit of Great Britain. London: J. Hatchard, 1802.

R. H. Timberlake, Jr. A critique of monetarist and austrian doctrines on the utility and value of money. Review of Austrian Economics, 1:81–86, 1987.

J. Tobin. Keynesian models of recession and depression. American Economic Review, 65(2):195–202, 1975. Papers and Proceedings of the Eighty-seventh Annual Meeting of the American Economic Association.

J. Tobin. Essays in Economics: National and International, volume 4. Cambridge, MA: The MIT Press, 1996.

R. M. Townsend. Models of money with spatially separated agents. In J. H. Kareken and N. Wallace, editors, Models of Monetary Economies, pages 265–303. Minneapolis: Federal Reserve Bank of Minneapolis, 1980.

R. M. Townsend. Economic organization with limited communication. American Economic Review, 77(5):954–970, 1987.

R. M. Townsend. Currency and credit in a private information economy. Journal of Political Economy, 97(6):1323–1344, 1989.

A. Trejos and R. Wright. Search, bargaining, money and prices. Journal of Political Economy, 103(1):118–141, 1995.

G. Tullock. Competing monies. Journal of Money, Credit and Banking, 7(4):491–497, 1975.

P. G. van Alfen. The 'owls' from the 1989 syria hoard, with a review of pre-macedonian coinage in egypt. American Journal of Numismatics, 14:1–57, 2002.

J. B. Van Huyck, R. C. Battalio, and R. Beil. Tacit coordination games, strategic uncertainty, and coordination failure. American Economic Review, 80(1):234–248, 1990.

T. Veblen. The preconceptions of economic science - part 1. Quarterly Journal of Economics, 13(4):396–426, 1899.

T. Veblen. The preconceptions of economic science - part 2. Quarterly Journal of Economics, 14(2):240–269, 1900.

T. Veblen. The limitations of marginal utility. Journal of Political Economy, 17(9):620–636, 1909.

T. Veblen. Essays, Reviews, and Reports: Previously Uncollected Writings. Edited by J. Dorfman. Clifton, NJ: Augustus Kelley, 1973.

T. Venturini and B. Latour. The social fabric: Digital traces and quali-quantitative methods. Proceedings of Future En Seine, pages 87–101, 2010.

L. von Mises. The Theory of Money and Credit. New Haven: Yale University Press, 1953.

L. von Mises. Money, Method and the Market Process. Edited by M. von Mises and R. M. Ebeling. Dordrecht: Springer, 1990.

S. Von Reden. The politics of monetization in third-century bc egypt. In A. Meadows and K. Shipton, editors, Money and its Uses in the Ancient Greek World, pages 65–76. Oxford, UK: Oxford University Press, 2001.

S. Von Reden. Money in Classical Antiquity. Key Themes in Ancient History. Cambridge, UK: Cambridge University Press, 2010.

F. A. Walker. Money. New York: Henry Holt & Co., 1878.

N. Wallace. General features of monetary models and their significance. In J. H. Kareken and N. Wallace, editors, Models of Monetary Economies, pages 251–260. Minneapolis: Federal Reserve Bank of Minneapolis, 1980.

N. Wallace. The overlapping generations model of fiat money. In J. H. Kareken and N. Wallace, editors, Models of Monetary Economies, pages 49–82. Minneapolis: Federal Reserve Bank of Minneapolis, 1980.

N. Wallace. Whither monetary economics? International Economic Review, 42(4):847–869, 2001.

N. Wallace. General features of monetary models and their significance. Mimeo, Swiss National Bank -Federal Reserve Bank of Cleveland Workshop on Monetary Economics, June 2002.

N. Wallace. The mechanism-design approach to monetary theory. In B. M. Friedman and M. Woodford, editors, Handbook of Monetary Economics, volume 3A, pages 4–24. Amsterdam: North-Holland, 2010.

L. Walras. Elements of Pure Economics or the Social Theory of Wealth. London: George Allen and Unwin Ltd., 1954.

L. H. White. Competitive payments systems and the unit of account. American Economic Review, 74(4):699–712, 1984.

L. H. White. Free banking in scotland before 1844. In K. Dowd, editor, The Experience of Free Banking, pages 157–186. London: Routledge, 1992.

P. H. Wicksteed. The Common Sense of Political Economy and Selected Papers and Reviews on Economic Theory. London: Routledge and Kegan Paul Ltd., 1933.

S. Williamson. Payments systems with random matching and private information. Journal of Money, Credit and Banking, 30(3):551–569, 1998. Comparative Financial Systems.

S. Williamson. Private money. Journal of Money, Credit and Banking, 31(3):469–491, 1999.

S. Williamson and R. Wright. New monetarist economics: Models. Research department staff report 443, Federal Reserve Bank of Minneapolis, April 2010.

L. Wittgenstein. Philosophical Investigations. Oxford, UK: Basil Blackwell Ltd., 1958.

K. H. Wolff. The Sociology of Georg Simmel. Glencoe, IL: The Free Press, 1950.

L. R. Wray. Understanding Modern Money: The Key to Full Employment and Price Stability. Northampton, MA: Edward Elgar, 1998.

L. B. Yaeger. Individual and overall viewpoints in monetary theory. In I. H. Kirzner, editor, Method, Process and Austrian Economics: Essays in Honor of Ludwig von Mises, pages 225–246. Lexington, MA: Lexington Books, 1982.

J. M. Zickgraf. Becoming like money: Proximity and the social aesthetics of 'moneyness'. Journal of Ethnographic Theory, 7(1):303–326, 2017.

A. Zimmern. The Greek Commonwealth. Oxford, UK: Oxford University Press, 1922.

Notes

[I] A question that mirrors the relationship between money and language, how people refer to money in casual, everyday conversation. Sohn-Rethel considers money "an abstract thing, a paradox in itself – a thing that performs its socially synthetic function without any human understanding" hence, it is "not related to our natural or physical being, but comprehensible only in our interrelations as human beings."[199] It leads Maurer to suggest, by implication, that if language is interior to the money form, then "it is difficult to say anything meaningful about money at all that is not immediately and already part of money itself."[200]

[II] The tension between the representation and the reality of money. In other words, the unseasy relationship between money's materiality (the stuff that money is made of as opposed to its signature; the metal instead of its coinage) and money's role in society. In recent years, technologists have jumped into this debate being forced, for the first time, to provide some form of justification for their idiosynchratic construction(s) of money.

[III] For the first time publicly announced on November 1, 2008, through a Cryptography and Cryptography Policy mailing list. It appeared as a new thread by one

[199] See Sohn-Rethel (1978, p. 45)

[200] See Maurer (2006, p. 16)

Satoshi Nakamoto under the heading *Bitcoin P2P e-cash paper* presenting "a new electronic cash system that's fully peer-to-peer, with no trusted third party" plus a link to the PDF version of a paper that developed the idea further. It also happens to be the first public reference to the `bitcoin.org` web domain. Some years later, Hal Finney (a well-known crypto-activist and active contributor to this forum) admitted that "[Satoshi] got a skeptical reception at best... [cryptographers] tend to have a knee jerk reaction."[201]

[IV] In August 22, 2008, Satoshi approached Wei Dai, nowadays a known figure to blockchain enthusiasts, asking him how to properly reference his paper on b-money. Strictly speaking it was not quite a "paper" but a post made in 1998 by Wei, then a computer engineering student, to the Cypherpunks mailing list. In that first contact, Satoshi mentioned knowledge of the b-money idea came from Adam Back, something that Back later admitted took place "when [Satoshi] emailed me about hashcash back in 2008." Nakamoto also provided Wei with a link to "a pre-release draft" of his paper, now seemingly "lost"; surprisingly enough, neither Wei nor Back admit in public to have kept a copy of that version. At the time, Nakamoto told Wei it had as title *Electronic Cash Without a Trusted Third Party* suggesting the birth of the term Bitcoin (or at the very least, it's first use in public) took place between August 22 and October 3, 2008. The latter date comes from the metadata of the "publicly available" version of the paper that Nakamoto released in November, having Bitcoin in its title (note the copy currently accesible from `bitcoin.org` has March 24, 2009 as timestamp; edits have been made to the latter version).

Perhaps noticing that Wei was unaware of Bitcoin's launch, as there are no records of Wei's participation in the Cryprography and Cryptography Policy mailing list since 2003, Satoshi contacted him by e-mail on January 10, 2009, to inform of the release of Bitcoin's protocol implementation through SouceForge. (From the available information, it is impossible to ascertain if they had other exchanges since Wei's reply to Satoshi's first e-mail.) Nakamoto also takes the opportunity to add, in passing, the code "achieves nearly all the goals you [Wei] set out to solve in your b-money paper."

[V] By Tim May's own account, he circulated the manifesto during Crypto '88 held at the UCSB Campus in August of that year. It seems that May did not present any paper during the event (collected for the LNCS edition 403, published in 1989) however he used the opportunity to distribute his manifesto to "like-minded people." It took a few years more, until the summer of 1992, for the Cypherpunk movement to formally emerge as "a loose federation of creative math hackers, civil libertarians, freemarket advocates, genius programmers, renegade cryptologists, and sundry other frontier folk"[202]

[VI] Following a search in the Web of Science and SCOPUS databases, neither the term blockchain nor distributed ledger show up in published academic papers before 2009. In fact, the first reference to a "blockchain" approach, then spelled as "block chain" (separate words; therefore it did not quite imply a new concept but more of

[201] See http://bit.ly/2Dnt107
[202] See Kelly (1994, p. 179).

an exemplification) appears in a late 1995 paper by Xiaofeng Han and co-workers published by the SIAM Journal of Computing.[203]

[VII]Reply to Sepp Hasslberger on February 15, 2009. The focus on central control is closely linked to the issue of privacy, of having to "trust them [institutions] with our privacy, trust them not to let identity thieves drain our accounts" (see previous quote in the main text).

On this subject, many years earlier Wei Dai posed a challenge on a debate that took place in the Cypherpunks forum. He wrote that "[just] because each individual wants more privacy for himself, it doesn't follow that everyone will be better off when everyone has more privacy."[204] It lead to a quite interesting exchange between Wei, Adam Back, Tim May and others.

Early on, Wei doubled-down on May by arguing that, if there is no particular reason for privacy to exist (May had added the phrase "Just say 'No' to 'Big Brother Inside'" to his e-mail signature) then, for all the feather ruffling around the issue, "it doesn't make sense to argue about the costs/benefits of privacy."[205] Shortly afterwards May admitted not to be arguing against privacy, but against "the validity of some of the attempts to 'prove' that privacy enhances markets..."[206]

[VIII]Hasselberg and other discussants in the thread created by Satoshi on the P2P foundation forum also noted that "stability of the coins' value is desirable for long term use." Interestingly enough, Hal Finney took a rather different perspective. Posting to the SourceForge Bitcoin list created by Nakamoto, on January 11, 2009 he wrote

> [o]ne immediate problem with any new currency is how to value it. Even ignoring the practical problem that virtually no one will accept it at first, there is still a difficulty in coming up with a reasonable argument in favor of a particular non-zero value for the coins.

He concluded, however, that if one took as value anchor the world's wealth "the possibility of generating coins today with a few cents of compute time may be quite a good bet, with a payoff of something like 100 million to 1!" Finney is not explicit but he's clearly using Household Balance Sheet data in his estimation.[207] This is an interesting take when compared to the view of Hasslberger and others.

[IX]Despite Nakamoto's efforts, Bitcoin's marketing actually began with Martti Malmi, then a young college student at Helsinki University of Technology that approached Satoshi in early May 2009.[208] Malmi announced himself as "Bitcoin Web Developer" in a post to the SourceForge mailing list in June 13, 2009. Changes in `bitcoin.org` design and positioning, however, appeared at some point between August 23, 2009 and January 6, 2010.

[203] See Han *et al.* (1995).
[204] Post on thread "'why privacy' revisited" dated March 21, 1997.
[205] Reply to Tim May on March 21, 1997.
[206] Reply to Adam Back on March 22, 1997.
[207] See, e.g. Davies, Lluberas and Shorrocks (2017, Table 6.3) calculated world wealth at $210.6 trillion in 2009.
[208] In Popper (2015, ch. 3).

[X]See the book by Goodway for an insightful analysis of the political positions and ideology defining these two very different groups.[209] He comments that "to replace 'anarchism' with 'libertarianism' and its derivatives would merely increase the confusion, especially now that right-libertarianism has appropriated them for anarcho-capitalism and laissez-faire minimal statism."[210] Newman focuses on the tension arising from the fact that, from an anarchist's perspective, "both positions –the minimal state (minarchist) and the no-state ('anarchist') positions– neglect the problem of economic domination; in other words, they neglect the hierarchies, oppressions and forms of exploitation that would inevitably arise in a laissez-faire 'free' market."[211]

[XI]Malmi publicly displayed his deeply rooted libertarian beliefs in a forum hosted at `anti-state.com` posting as *Trickstern* (username adopted by Malmi, registered on April 9, 2009). Prior to contacting Nakamoto, he created a thread about Bitcoin under the heading *P2P Currency could make the government extinct?* to which later Satoshi, on some occasions, also contributed. Interestingly enough, the `anti-state.com` forum (plus a blog also hosted there) acted as a cog of the "Project for the New Anarchist Century" promoted by a US-based religious anarchist group having deep Evangelical roots.[212]

Whether they knew at the time, or would have cared if they knew, is another matter.

Nakamoto in fact made it clear he was not of the anti-capitalist type. "I don't care if wealth is concentrated..." replied once Satoshi to Laszlo Hanecz, the first person that in 2010 managed to use bitcoins for a real-world purchase: two Pappa John's pizzas delivered to his home in Jacksonville, Florida (in Popper, op.cit., ch. 4).

[XII]Underlined mine. Contrary to Zooko's perception it was silver, rather than gold, the metal that predominated since the first coins were struck post 550 BC.

In ancient Mesopotamia (using a broad brush to denote the cultures established between 3200 BC to about 300 BC in or neighbouring the region of modern Iraq) silver was plentiful, although it was not a native metal and had to be imported. Gold was more abundant in ancient Egypt, particularly so after control of the Nubia region. Precious metals had extensive non-monetary use in both geographical domains, but silver was more widely available. In villages, e.g. like Deir el-Medinah metals were used to establish value rather than to effect transactions, and a specific term, "his silver," (reflecting the dominance of this metal) emerged as a colloquial way to refer to the value of goods.[213]

To no surprise then, silver became the metal used mostly as money. Quoting Smith, Einzig tells about the usage in Cappadoccia of silver ingots stamped by State authority for commercial transactions.[214] That said, accounts by Herodotus

[209] See Goodway (2011).
[210] Ibid., p. 335.
[211] See Newman (2010, p. 43, note 30).
[212] See Christoyannopoulos (2009).
[213] See Kemp (2006).
[214] Op.cit., p. 209.

trace the introduction of coinage to the *stater* coin (made of *electrum*, an alloy of gold, silver and copper) of the Lydian kingdom. The capital of Lydia, Sarded, had a thriving trade by land with Babylon and the *stater* could be interpreted as Lydia's "domestication" of the Babylonian *mina*.

Einzig nevertheless pushes the argument that Cappadoccian silver ingots "differ from the golddumps produced by the King of Lydia 1,500 years later in degree only" and therefore "credit for the invention of State-guaranteed money must be given to Cappadocia."[215]

Be that as it may, the subsequent expansion of coinage to Greece is due to the Phoenicians rather than the Babylonians. They excerted a dominant influence in the Greek world, leading to the gradual introduction of their silver standard; incidentally, the Phoenicians were the first to exploit at scale the silver mines in Tamasus, Thasos and locations in Spain, particulary Rio Tinto.[216]

Coinage in Greece, and the monetisation of its economy, cannot be understated. In Ionia, a rather small hoard of coins, 900 pieces attributed to archaic Colophon, revealed its importance. Those 900 coins were seemingly produced by about 400 different dies; hence "if we were to assume very conservatively that a die could only produce 1000 to 5000 coins in its lifetime, the scale of the minting would still range from hundreds of thousands to millions of pieces."[217] For coins that are presumed were only used locally, "[the implicit] volume of coinage is impressive and is also suggestive of a strong local requirement for low denomination coins."[218]

Still, even in the Roman society there was no uniformity as to considering only coins as money. Plinius, in *Naturalis Historia* mentions early Roman money to consist of bullion circulating by weight rather than tale. There are a number of provisions in the Justinian Digest and Code on salaries, legal threshold values, fees and fines, expressed in weight of gold and silver rather than coins. Although the Roman Empire by 100 AD relied on a bimetallic coinage system (or trimetallic if we consider small-change coins made from brass, bronze or copper) as late as 367 AD the rules for tax payments stipulated their payment to the Treasury had to made in bullion.

Regular gold coinage in Rome started around 46 BC, although Tacitus points out that for small transactions only silver coins were used.[219] Egypt, running a closed monetary system, used the silver *tetradrachm* struck in Alexandria since the days of Ptolemy I (General and boyhood friend of Alexander).[220] There is ample evidence suggesting gold coins were used when large sums needed to be transported, and for large transactions.[221] In any case, gold as dominant coinage metal had to somehow "wait" until Constantine I promoted the widespread adoption of the gold *solidus*

[215] Ibid., p. 210.
[216] In Markoe (2000).
[217] See Kim (in Cartledge, Cohen and Foxhall eds., 2002, p. 47).
[218] Ibid.
[219] See Tacitus (in Rodney Potter 1935, 5.3-5).
[220] Although a silver standard was already in place by the end of the New Kingdom. In Manning (2006, p. 5).
[221] See Sperber (1974, p. 89).

(shilling) that replaced the old *aureus* after 312 AD.[222] By the late third century, the silver *denarii* saw its fitness greatly reduced (debasement) until its minting stopped completely. Although some attempts were made to re-introduce a silver currency, by the end of the fifth century silver coins almost completely dissappeared.

The *solidus* dominance however lasted until 755 AD, when Pepin the Short introduced the silver *novus denarius* (penny) that brought an end to gold minting; the solidus was only kept as a paper unit of account, equal to 1/20 of a *librum* –pound– divided into 12 denarius.

The silver penny became the coin typically produced by mints throughout medieval Europe. In the 13th century, the "moneta grossa" (a similar, but slightly heavier coin than the silver penny) was struck by Italian city states, and not much later mints began to introduce gold coins such as the Florentian *florin* in 1252 or the Venetian *ducat* in 1284, both circulating alonglside the *denarius* now referred to as "moneta minuta" (or more colloquially, *piccolo*).

The proper re-introduction of a gold standard took much more time to materialise. So, e.g. despite becoming *de facto* (because of the impact on metal flows) in the United Kingdom after the 1696 Coin Act and the subsequent 1774 recoinage, it only became *de jure* in the 19th century after the Napoleonic wars. Quoting Thomas Smith once more,

> [Locke's] disciples in England of the present day... have adopted gold, and with their usual consistency they quote him as in their favour, although he has positively declared *that gold neither was the money of the world or the measure of commerce, nor was it fit to be so*.[223]

In any case, looking back and judging by its permanence, gold standard "experiments" have been rather transitory, relatively short-lived arrangements throughout monetary history.

[XIII]Temple vowed by M. Furius Camillus during the war with the Aurunci in 345 BC and dedicated in 344 BC.[224] The mint was relocated there (some accounts say from the Temple of Saturn) during the last centuries of the republic, perhaps in 269 when silver coinage (which could be purchased for bullion) was introduced into Rome.[225]

The mint stood in the Juno temple for nearly four centuries, yet some scholars argue that "the affair of striking money was likewise performed in other temples and under other patronages."[226] Unfortunately, there are no surviving mint records from Roman times.

[222] See Hendy (1985) although there is some debate as to the correct name; some authors, e.g. Klose (in Cancik and Schneider, 2001) provide evidence as to the *aureus* being the "new" coin.
[223] See T. Smith 1832, p. 26.
[224] See also Cicero, *On Divination* (1923, 1.101).
[225] See the account by Ball Platner and Ashby (1929, pp. 289-290); also Bayle (1736, p. 639).
[226] See Stukeley (1757, p. 85).

[XIV] The usage here of the term "pure barter" is an attempt to differentiate the situations where (quite likely a primitive) society had no form of money or currency, and where no commodity, amongst those available for exchange, had been "found" to fulfill the role of money. It is a rather different context to the conditions leading to (organised forms of) barter despite the existence of money, commodity or fiat-based. For example, the conditions post-2001 crisis in Argentina[227] or the emergence of cigarette money in Europe post World War II.[228]

[XV] In Walras the coincidence of wants problem arises as a result of the division of labour.[229] Some agents (entrepreneurs) specialise in production and others (labourers, landowners and capitalists) in consumption. Einzig, acknowledging the gap between barter and modern money "is very wide" also notes that

> [t]here is no reason to suppose that the absence of modern money hindered considerably the development of a rudimentary division of labour or the earliest phases in the emergence of a capitalist production. A certain degree of division of labour was already possible even under barter, and the use of money, however primitive, encouraged and facilitated further specialization.[230]

Although money to Walras bears no direct utility, it performs a buffer role due to the lack of synchronisation, in any given exchange period, between the moment in which agents are "paid" relative to the moment they want to "spend" as a consequence of delays in production (the process of converting raw materials to end products). A proposed solution to the double coincidence of wants problem due to Clower is the imposition of a cash-in-advance constraint,[231] a specific form of transaction technology, as used by Lucas or in search models (which effectively endogenise Clower's constraint) as in Kiyotaki and Wright.

[XVI] Wallace considers that "monetary trade is essential in the sense that some good allocations are implementable using monetary trade that would otherwise not be implementable."[232] Going back to Menger and Walras, explaining the "essentiality" of money becomes a slippery slope at this stage simply because they adopted different approaches to the issue of money. The only thing that "connects" both authors is their treatment of money purely as a medium of exchange.

[XVII] The reference to metals, perhaps, provides the narrowest construction of a medium of exchange emerging as a market response to the problems posed by barter. Writing about Aristotles' *Politics*, Schumpeter makes the point that "in order to serve as a medium of exchange in the markets of commodities, money itself must be one of these commodities."[233] It follows that becoming a medium of exchange has nothing to do with a commodity being metallic or not. Still, Aristotles goes one step further, arguing that gold or silver perform this function much better than other commodities.

[227] In, e.g. Gomez (2016)
[228] In Burdett, Trejos and Wright (2001) or Bignon (2009).
[229] See Walras (1954 [1926], part IV, lesson 29).
[230] Ibid., p. 486.
[231] See Clower (1967)
[232] See Wallace (2002, p. 2).
[233] See Schumpeter (1986 [1954], p. 60).

Metallism takes this idea and pushes it to the extreme. To them, "the value of a currency depends on the intrinsic value of the gold, silver or copper it is made of, or which backs a note issue."[234] Coinage, the simple act of "putting a stamp" on metal is assumed to be just a matter of convenience.[235]

In that sense, Aristotles makes it clear in his *Ethics* that money is the child of custom,[236] not something that emerges naturally, and hence

> this is why money is called *nomisma*, because it exists not by nature but by convention (*nomos*), and it is in our power to change its value and to render it worthless.[237]

There is no reason, of course, to believe there is an apparent contradiction: one thing is to speak about what led to a commodity becoming money and another what's the "perceived" value of said commodity (quite evidently, in Aristotle's ontology of money perceptions lead to a certain "custom" becoming adopted). Where there is indeed a difference is in the "services" that money renders as a result of its social acceptance, and consequently the power given to institutions (where society is, or ought to be, "represented") to change things.

Some authors position Locke as a hardline Metallist before Menger. Locke, however, was never concerned about the origin of money, only stating that it happens to be a (precious) metal, in this case silver. He wrote "the *quantity* of pure Silver separable from the Alloy, makes the real *value* of Money"[238] but also "[t]he intrinsic value of Silver considered as Money, is that estimate which common consent has placed on it"[239] so he merely observes the fact that a precious metal was made money by convention, rather than attempting an explanation as to why that might have been the case. Perhaps a clue as to this quite dogmatic position can be found in Locke's view on credit, which he deemed a temporary arrangement and quite different from money. To wit,

> Money is necessary... [f]or where money failes, men cannot buy and Trade stops. Credit will supply the defect of it to some degree for a litle while. But Credit being nothing but the expectation of Money within some limited time, money must be had or credit will faile.[240]

[XVIII] The Austrian and neoclassical traditions are frequently assumed as synonymous, and how they are popularly associated, but that's far from being the case. As Jaffe pointed out, the works of Jevons, Menger and Walras are far less homogeneous than otherwise thought.[241]

---

[234] As in Rutherford (2002, p. 381).
[235] See Schumpeter (op.cit., p. 60).
[236] Jevons once wrote "some one article will usually be selected, as *money par excellence*, by custom or the force of circumstances." In Jevons (1919, p. 13).
[237] In Aristotle (2004, ch. 5, p. 90).
[238] See Locke (in Kelly 1991, p. 311).
[239] Ibid., p. 410.
[240] Ibid., p. 379.
[241] See Jaffe (1976).

The founding members of the Austrian School (Menger, Böhm-Bawerk and Wieser) of course resorted to marginal analysis; in fact, it was Wieser who invented the term "marginal utility" or *Grenznutzen* as an alternative to Jevon's notion of final degree of utility.[242]

The Austrian School, however, took a radical turn with Hayek, one of Wieser's disciples. Best characterised as a "rediscovery" of Menger, it is a shift that can be traced back to Hayek's 1936 presidential address to the London Economic Club[243] and his questioning of the meaning and use of neoclassical equilibrium, perhaps not being fully aware at the time of its implications. Recall that Menger, contrary to Jevons and Walras, disagreed with the assumption that the agents' optimally chosen plans[244] must be compatible, giving rise to an equilibrium state.

A proper exposition of the rift that subsequently opened with the Neoclassical School goes beyond the scope of this paper.

In any case, saying the methodological approach of marginalists and early Austrians had many points in common is indeed correct. So much so that Veblen linked the Austrian and Neoclassical schools using "utilitarian hedonism" as caption.[245] The "revision of [the] hedonistic dogma"[246] marked by the analytical shift from production towards consumption taking place since Smith, according to Veblen. It was clearly not about ethics[247] but about hedonism going all the way towards providing an empirical explanation of human nature.

[XIX] Knapp suggested that

> [perhaps] the Latin word "Charta" can bear the sense of ticket or token, and we can form a new but intelligible adjective – "Chartal." Our means of payment have this token, or Chartal, form. Among civilized peoples in our day, payments can only be made with pay-tickets or Chartal pieces. (op.cit, pp. 32-33)

In Latin, *charta* is a "paper made from papyrus"or simply "a material for writing."[248] Going slightly forward into the discussion presented in Section 4, the Chartalist view "is not preoccupied with the medium of exchange function of money. On the contrary, Chartalist theory seeks to uncover the essential properties of money as a unit of account and a means of payment."[249]

[XX] It might prove useful to highlight the notion of "access costs" as slighly separate from that (although a subset) of "transaction costs." The former were typically reflected in the difficulties people had to access foreign-denominated currency (e.g.

[242] See Marshall's *Principles* (2013 [1890], book I, p. 79.1 and Appendix, p. 690) where he translated Jevon's term as "marginal degree" of utility.
[243] See Buchanan and Thirlby (1981).
[244] By maximising their objective function –that is, their utility function– subject to a budget constraint
[245] See Veblen (1973).
[246] See Veblen (1900, p. 243).
[247] As Marshall attempted to show, in defense (op.cit., book I, ch. 2, p. 70n).
[248] See Oxford's Latin Dictionary (1968, p. 309) and also Cassell's (1953, p. 800). It is also expressed as "Cartalist."
[249] See the paper by Bell (2001, p. 154).

time spent, practical access to the black market) whereas the latter simply mirrored the ability to use such currency in commercial transactions (many were only feasible if foreign curency was involved in the exchange, cases where foreign money was the only liquid asset). Although the cost of acquiring an asset is indeed a transaction cost in a classic sense, during hyperinflations two phenomena tend to manifest themselves: that of currency procurement (mostly informal outlets that people use to convert local money into foreign currency) as a separate layer from the circulation sphere (where transactions using foreign currency became the norm). It was not unusual for foreign currency to make several "rounds" before being "converted back," e.g. someone along the chain having to fetch local currency to pay taxes, say.

XXI This was also emphasised in a paper by Abba Lerner published in the *American Economic Review*. He wrote that

> [T]he modern state can make anything it chooses generally acceptable as money and thus establish its value quite apart from any connection, even of the most formal kind, with gold or with backing of any kind. It is true that a simple declaration that such and such is money will not do, even if backed by the most convincing constitutional evidence of the state's absolute sovereignty. But if the state is willing to accept the proposed money in payment of taxes and other obligations to itself the trick is done.[250]

Or, in the words of Knapp, "the money of the state is not what is of compulsory general acceptance, but what is accepted at the public pay offices."[251] Hence, being a "legal tender" is not of the essence. It also leads, quite directly, to a notion of sovereignty defined by "the power to tax and collect in the token of choice."[252] Service value is not a perception, but comes by enforcement.

In an interesting pamphlet published in the United States in 1832, one Thomas Smith wrote

> [have] not all governments retained the power not only of determining what is to pass exclusively as money, but also the value at which it is to pass?[253]

It is very clear the ideas outlined by Knapp already had some traction.

XXII Two influential works, his much quoted *Metropolis and Mental Life*[254] and his *Philosophy of Money* were published in between Menger's *Principles* and Mises *Theory of Money and Credit*. The influence of Menger on Simmel has been widely acknowledged.[255] Mises takes stock from Simmel's notion of exchange as an essential feature of human action ("every economic act may be regarded as a kind of exchange," op.cit., I.2.2) and as the cornerstone of a theory of value.

Yet, contrary to Menger and other contemporaneous economists, Simmel does not engage, nor wants to engage, in any sort of economic theorising.

---

250 See Lerner (1947, p. 313).
251 See Knapp (op.cit., vii)
252 In Rochon and Vernego (2003, p. 58).
253 See T Smith (1832, pp. 28-29).
254 See Wolff (1950).
255 In e.g. Laidler and Rowe (1980, p. 98).

> Not a single line of these investigations is meant to be a statement about economics. That is to say, the phenomena of valuation and purchase, of exchange and the means of exchange, of the forms of production and the values of possession, which economics views from *one* standpoint, are here viewed from another.[256]

[XXIII] Berkeley wrote *The Querist* in a particular form, using questions or queries that he blended in a somewhat messy way. Still, on the question of money, Berkeley first asks

> Whether money be not only so far useful, as it stirreth up industry, enabling men mutually to participate the fruits of each other's labour?[257]

and as follow-up, asks

> Whether money is to be considered as having an intrinsic value, or as being a commodity, a standard, a measure, or a pledge, as is variously suggested by writers? And whether the true idea of money, as such, be not altogether that of a ticket or counter?[258]

To Berkley, then, money could be "tickets or tokens for conveying and recording such power"[259] and what (physically) makes those tickets or tokens has no practical consequences.

[XXIV] Taking stock from Bohannan's "spheres of exchange" concept, developed during his study of the Tiv people in central Nigeria.[260] In the multi-centric economy of the Tiv, Bohannan identified three spheres: one associated to subsistence; a second one considered the prestige sphere, largely similar (in terms of the goods involved in exchange) to what the Greeks called *pecunia*; and finally a kinship sphere.

Influenced by Polanyi,[261] Bohannan introduces the concepts of general-purpose and special-purpose money as distinct categories. The former was used for multiple functions, the latter only used within the specific spheres of exchange.

In separating the modern and pre-contact organisation of Tiv's society, Bohannan makes a case for the flattening of the complex, sometimes dense networks of value formation (built on distinctions of rank, age and gender) brought by the introduction of colonial money.

> [the] early Administrative officers interpreted [Tiv] brass rods as "money," by which they meant general-purpose money. It became a fairly easy process, in their view, to establish by fiat an exchange rate between brass rods and a new coinage, "withdraw" the rods, and hence "replace"one currency with another. The actual effect, as we have seen, was to introduce a general purpose currency... yet Tiv constantly express their distrust of money... [both facts] have broken down the major distinctions among the spheres.[262]

[256] See Simmel (1907 [2004], pp. 54-55).
[257] See Berkeley (in Luce and Jessop eds. 1953, p. 105.5).
[258] Ibid., p. 106.23.
[259] Ibid., p. 107.35
[260] See Bohannan (1959, pp. 491-503); also Sillitoe (2006).
[261] In Polanyi (1944, p. 492).
[262] In Bohannan (op.cit., pp. 500-501).

Bohannan notes an important collateral effect of this transformation of the Tiv into a "unicentric" economy, due to the fact that values remained unchanged. Of particular importance was the Tiv's "value of maximization, converting one's wealth into the highest category, women and children."[263] As the access to and circulation of colonial coins (general-purporse money) increased, brideprice started to feel the impact of inflation. He notes

> [the] number of women is limited... rights in women have entered the market, and since supply is fixed, the price of women has become inflated.[264]

Other authors have also reported the interaction between, e.g. cowrie shells in West Africa and colonial (coined) money.[265] Dalton argued that as colonial money found its way to settle non-commercial uses, such as bridewealth, they led to "inevitable repercussions on traditional social organization and cultural practices"[266] showing the impact of general-purpose, "universally solvent" money in regulating social relationships.[267]

Still, challenges to the view that money "flattens"social relations come from the sociological camp[268] suggesting that money (and finance) perhaps create new forms of social relations, possibly as complex as the ones they substitute.

[XXV] Keynes noted Innes' train of thought followed that of H. Dunning Mcleod credit theory of money.[269] Mcleod carried forward the debate about the pervasive use credit going back to Henry Thornton.[270] Schumpeter wrote that

> from the fourteenth and fifteenth centuries on (and even in the Graeco-Roman world) the gold or silver or copper was the familiar thing. The credit structure –which moreover was incessantly developing– was the thing to be explored and to be analyzed.[271]

Mcleod, in the same way as Menger, noted the difficulties in barter[272] arising from exchanging commodities or services of unequal value, but unlike Menger[273] in such cases "there would remain a certain amount of product or service due from the one

[263] Ibid., pp. 502.
[264] Ibid.
[265] Hogendorn and Johnson (1986) or Graeber (2001).
[266] In Dalton (1965, p. 61).
[267] See, e.g. Piot (1991).
[268] See, e.g. Keister (2002)
[269] See Mcleod (1882, 1889).
[270] See Keynes (1914); this issue was also tackled by the likes of Fullarton, Tooke and J. Stuart Mill.
[271] In Schumpeter (op.cit., p. 686)
[272] Mcleod wrote "the inconvenience of this mode of trading is palpable" (1882, lecture II, p. 42).
[273] Menger, in his quest for explaining the emergence of a commodity that can be used as an acceptable medium of exchange (and thus solve this issue) proposes his theory of saleability (or *absatzfähigkeit*) of goods; those goods "[whose] possession would considerably facilitate the individual search for persons who have just the goods he needs." (See Iwai, op.cit., p. 397).

to the other“ constituting a debt, and at the same time “the corresponding duty created on the person of the other who had received the greater amount to render the balance due when required.”[274]

Concluding his review of Innes, Keynes wrote

> [t]he main historical conclusions which [Innes] seeks to drive home have, I think, much foundation, and have often been unduly neglected by writers excessively influenced by the 'sound currency' dogmas of the mid-nineteenth century. Not only has it been held that only intrinsic-value money is 'sound', but an appeal to the history of currency has often been supposed to show that intrinsic-value money is the ancient and primitive ideal, from which only the wicked have fallen way. Mr. Innes has gone some way towards showing that such a history is quite mythical.[275]

[XXVI]On the opposite sidewalk, institutionalists place those that consider money to be primarily an instrument (medium of exchange) considering them, by extension, as forming an Instrumentalist School.

The epithet “institutionalist” in this context is mostly attributed to Dudley Dillard, a fervient advocate of the claim that money is an institution (or perhaps more accurately, of money as an institution). In his own words, money is “the key institution of contemporary capitalism”[276] although he duly credited Marx as “the original institutionalist.”[277]

That said, there remains the non-trivial question of how to define institutions. Hogdson notes that “even today, there is no unanimity in the definition of this concept.”[278] Some precedents can be found, however, in what Walton Hamilton defined as “Institutional Economics”[279] and the guidelines offered ten years earlier by Veblen, who wrote that institutions are “the settled habits of thought common to the generality of man.”[280] Wesley Mitchell, in turn, suggested institutions are “merely a convenient term for the more important among the widely prevalent, highly standardized social habits.”[281]

On account that institutions are perceived as covering a broad spectrum of social interactions, Hogdson (along Mitchell's lines) has stated the most comprehensive definition of institutions available, as “systems of established and prevalent social rules that structure social behavior” hence “[l]anguage, money, law, systems of weights and measures, table manners, and firms (and other organizations) are thus all institutions.”[282]

---

[274] Ibid., p. 43.
[275] Keynes (ibid., p. 421).
[276] See Dillard (1984, p. 421).
[277] See Dillard (1987, p. 1644).
[278] In Hogdson (2006, p. 1).
[279] See Hamilton (1919, pp. 308-318). It should be stressed that Hamilton provided the most convoluted definition of institutions yet, so it will not be entertained here.
[280] See Veblen (1909, p. 626).
[281] See Mitchell (1924, p. 25).
[282] In Hogdson (ibid., p. 2).

Nowadays, perhaps the closest link between economics and institutionalists (on issues of money and credit) can be found in the Post-Keynesian School.[283]

XXVII It might be useful to explain what is understood by "coordination" here. The best way to do so is by first showing cases of coordination failures.

Let's assume John is a butcher and Julia wants to buy some meat for a barbecue. If Julia heads to the butcher's shop only to find it closed because John decided to stay at home that day, then we have a coordination failure. Consider, as another example, the so-called "battle of the sexes" game. Julia and Ed decide to meet one evening yet they cannot remember if they planned to go to the opera or to watch a football game; Julia would prefer the opera, Ed the football match but both would like to do something together. Clearly a sticky wicket.

A coordination game is any game that exhibits multiple, Pareto-rankable Nash equilibria, including games in which the players have no identical preferences over the set of outcomes.[284] The above examples show cases where multiple equilibria could indeed be a possibility, situations where no single individual sees an incentive to deviate if others conform to the outcome.

So, for example, in the battle of the sexes game Ed might agree to go to the opera because he is certain Julia will be there although he would prefer both to be seeing the football game.

Why is it relevant? One of the issues with money (and also credit, incidentally) is that it requires a particular coordination of beliefs. If that does not take place, meaning that agents are free to form any beliefs as to what other agents in the economy will do, the end result is autarky.

XXVIII The use of the "primitive form" qualifier is not casual. Modern technology[285] can nowadays ensure that individuals stay within their budget constraints,[286] an essential by-product from the use of physical money or of barter.[287] In that respect physical money is deemed a primitive, simple functional equivalent.

Therefore, following the argument set forth by Wallace (2010) imperfect monitoring is a necessary condition for money to be "essential." In other words, in an economy with perfect monitoring the existence of money does not enlarge the set of implementable allocations.[288]

The rationale is simple to grasp. Money is assumed to be accepted because the following takes place.

---

[283] In Arestis and Eichner (1988), Arestis (1992) or Lavoie (2014), to cite a few.

[284] See, e.g. Cooper *et al.* (1990; 1992a,b); Van Huyck *et al.* (1990)

[285] As Searle (1995, p. 56) argued, "a blip on a computer disk."

[286] Meaning that it is impossible for anyone to spend beyond their money holdings or credit limit using plastic or most electronic means of payment.

[287] Whether an individual has borrowed, stolen or found a dollar bill on the street is irrelevant. What matters is that it can be rapidly (and it could be added, cheaply) verifiable.

[288] Kocherlakota, however, presents in his 1998 paper an example showing his main result does not hold if perfect monitoring replaces memory (perfect monitoring meaning: knowledge of the past actions of all players and not just that of direct and indirect trading partners).

- Frictions (typical of a market economy) are eliminated by using money; and
- As higher welfare is attainable by overcoming such frictions, every agent "expects" every other agent to accept money in an exchange.

Compliance (ensuring such expectation is met in practice) requires finding a way to exclude those agents that are not happy to accept money; to do so, information about past transactions is necessary. Since trade information is private, a mechanism needs to be in force for it to become publicly accessible. Say, a data bank.[289]

Given that such monitoring is assumed to be costly then such data bank becomes complex to implement. Others argue that monitoring only needs to be "sufficiently limited" for money to become essential.[290]

Money would not be essential, however, if there are functional and feasible alternatives to it. Credit is one such alternative, which, in addition, strictly dominates money on efficiency grounds. Why? Because credit decorrelates agent's consumption and monetary holdings. That said, there is a trade-off between efficiency and coordination: although credit might be more efficient, agents might find they coordinate better on money.

XXIX The issue of bitcoin deflation (also applicable to other cryptocurrencies of similar design) has become, for many outside of the groups of die-hard converts, one of its most controversial facets. Unfortunately, pretty much every organic debate taking place around this topic tends to be driven, as mentioned earlier, by popular beliefs.

To properly understand the (potential) implications of a deflationary currency, however, one has to look into one of the key stylised facts of economics: price/wage stickiness. In itself not an easy task, because (in particular) the notion of wage stickiness has itself been a contested topic amongst economists, despite its apparent empirical suppport. Those in the *New Classical* camp dismiss wage stickiness as unimportant or non-existent, attributing cyclical fluctuations in employment to high rates of intertemporal substitution of labor as a response to changes in labor productivity, whereas *New Keynesian* economists argue that the (downward) stickiness in nominal wages is precisely what prevents an economy from maintaining its employment level in the face of shocks to aggregate demand or supply.

Back in 1802 as he developed his case about the "pressure on the mercantile world" brought by adverse supply shocks, Henry Thornton wrote

> a fall arising from temporary distress, will be attended probably with no correspondent fall in the rate of wages; for the fall of price, and the distress, will be understood to be temporary, and the rate of wages, we know, is not so variable as the price of goods[291]

that being the reason why he believed, contrary to Ricardo, that monetary contraction was not an adequate response. Because of nominal wage stickiness he vigorously argued that

[289] Or mandating that agents "reveal" their money holdings, as in Wallace (2000).
[290] See Calvacanti and Wallace (1999).
[291] In Thornton (1802, p. 82).

> [a] diminution in the price of manufactures... may also, if carried very far, produce a suspension of the labour of those who fabricate them.[292]

Since then lots of water passed under the bridge. More recently than Thornton's observation we have, e.g. Ball and Mankiw's famous 1994 NBER sticky-price manifesto or also Basu, Fernald and Kimball's 2004 NBER paper on technological change, the latter showing that if prices are (even slightly) sticky innovation bursts generally lead to a decline in input use and investment demand in the short run.

All said, some economists feel the case for price stickiness is not clear-cut, because there is the distinct possibility that even in an economy where prices are fully flexible, macroeconomic fluctuations might still appear (in other words, price stickiness is a sufficient but not necessary condition driving business cycles). Tobin made the case in a largely neglected paper published in 1975 by the Cowles Foundation (appearing later in the AEA 1975 Proceedings).

> Keynes tried to make a double argument about wage reduction and employment.[293] One was that wage rates were very slow to decline in the face of excess supply. The other was that, even if they declined faster, employment would not – in depression circumstances– increase. As to the second point, he was well aware of the dynamic argument that declining money wage rates are unfavorable to aggregate demand. But perhaps he did not insist upon it strongly enough, for the subsequent theoretical argument focused on the statics of alternative stable wage levels.[294]

So, at the end of the day, if wages are more resilient to downward pressures relative to other prices in the economy in periods of weak demand, real wages will move countercyclically (on aggregate). Although the empirical evidence is somewhat mixed, the available data suggests that's precisely the case at least for developed economies. Money, using the economists' parlance, is not neutral.

What are the implications for a "deflationary" currency? In the presence of wage stickiness, deflation in the unit of account would lead to unemployment. That, in turn, is what will keep it from displacing traditional currencies.

XXX The idea of sequential economies was proposed years earlier by Lindhal (1939) and Hicks (1939) in a general equilibrium (Walrasian) context. The basic difference is that in Hicks-Lindhal agents make consumption plans based on expectations of future prices of commodities, whereas Radner proposed an equilibrium based on plans, prices and price expectations (so requiring agents to have perfect foresight).

Sequence economies provide an alternative to the Arrow-Debreu world,[295] that is, one having an economy with a complete set of future markets. Why is that relevant? Because the Arrow-Debreu model is the one that most acurately captures the Smithian view of market economies. In other words, one where the "Invisible Hand" performs flawlessly.

---

[292] Ibid., p. 81.
[293] He devoted chapters 19 to 21 of his *General Theory* to develop a sticky-wage explanation of unemployment. See Keynes (1964).
[294] See Tobin (Cowles 1975, pp. 2-3).
[295] See Arrow and Debreu (1954).

This economy, however, does not require money. For money to have a role, markets for future goods or future contingent goods must be missing. This critique (the inability of an Arrow-Debreu economy to find a role for money) was first laid down by Hahn (1965). Hahn started from an obvious, simple observation: "actual economies do use money." Consequently, "it is an open question whether actual market economies can deliver what Smith and the modern market advocates claim for them."[296]

XXXI It became known as the "Hahn Problem" and about money not quite finding a "place" in a Walrasian economy. The controversy can be traced to Patinkin's attempt at redrawing of the quantity theory in his 1956 classic *Money, Interest and Prices*.

As a very quick summary, developing on the Walras-Hick tradition, Patinkin's strategy to model the transactions role of money was to "force" real balances into the utility function, and in that way treating money like a commodity.[297] Hahn's critique, in turn, had two sides to it. Firstly, he argued Patinkin's framework did not explain why people would be willing to hold money when it is dominated by other assets in terms of return. Secondly, that it was a poor attempt at solving the non-existence of a monetary equilibrium (positive demand for money).

Hahn's reasoning started from a simple premise: in a Walrasian (Arrow-Debreu) framework, an equilibrium will always exist where fiat money has no intrinsic value, but, if that is indeed the case, then money cannot play the role of a means of exchange. Or, put in a slightly different way, barter equilibria cannot be completely excluded (as the monetary equilibrium can be matched to a barter equilibrium where nobody attaches value to money). Therefore, the "problem" is to find whether an equilibrium can still exist if money has otherwise a positive value.

Keynes wrote in his *General Theory* that "the fact that contracts are fixed, and wages are usually somewhat stable in terms of money, unquestionably plays a large part in attracting to money so high a liquidity premium."[298] Hahn argued such liquidity premium arises when "the expected gain in welfare of holding an extra unit of a non-monetary asset must exceed the expected gain on a unit of money, if the non-monetary asset is to be held."[299] Therefore, in Hahn's "problem" an equilibrium in which the liquidity premium of fiat money is zero cannot be ruled out, in which case the economy reverts to barter.

That said, Hahn's problem is also *relevant to commodity money*. For example, gold might be adopted as a medium of exchange and still command a liquidity premium despite the fact that its intrinsic output value is positive (unlike fiat money).

XXXII There are start-ups looking at linking plastic money to crypto-currencies. How does it work? By using the infrastructure of an electronic payments provider, such

[296] See, e.g. Hahn (1989, pp. 7-8).

[297] See Patinkin (1965 [1956]). The term "problem" emerged following Hahn's famous 1965 critique. Patinkin's work, taken in the context of postwar economics, can be seen as an attempt to "rescue" the quantity theory of money from Lange's and Keynes' attack.

[298] See Keynes (op.cit., ch. 17, p. 236; underlined mine).

[299] See Hahn (1989, p. 11).

as Visa or MasterCard, to link POS card readers to a cryptocurrency exchange. It requires the user to carry a crypto-enabled plastic card that is identical (in every respect) to the plastic debit card issued by any high-street bank, but linked to the virtual wallet you use to store bitcoin or other cryptocurrencies.

Say you go to your favorite store and make a purchase, using this new plastic card for payment. Once the merchant swipes the card, the network checks the exchange rate between the cryptocurrencies the buyer owns and a legal tender, converting the price of the purchase at that rate and debiting from the buyer's wallet the required number of coins. To pay the merchant, the exchange trades the coins it has debited from the purchaser's wallet and pays the sales price into the merchant's Visa or MasterCard account, after deducting any interchange fees. The card operator makes money by taking a cut (negotiated with Visa or MasterCard) of those interchange fees.

To run in real-time, however, the whole operation requires a separate infrastructure on top of the existing crypto-currency one. Simply put, a transaction confirmation time of even a few minutes is not realistic in a POS environment. It also requires one, or multiple, liquidity providers to convert from one blockchain asset to another.

On Cryptocurrencies – Seven Years Later

Eduardo Salazar
Forctis AG

February 2025

This paper was conceived in 2018 as a thought-provoking primer on cryptocurrencies, blending historical depth with theoretical insight to frame Bitcoin both as a reaction to the Global Financial Crisis and as a monetary experiment.

The aim was to characterize cryptocurrencies (exploring *what they are* and *what they could become*) using history, economic theory, and sociology as primary tools. A historical-critical work rather than a quantitative or mathematically oriented one, it weaves a narrative connecting Bitcoin's emergence to monetary evolution, tracing its way from ancient coinage to Nakamoto's forum posts.

Directed mostly directed at policymakers, historians, or crypto enthusiasts seeking context, not models or equations, this piece was meant as a scene-setter.

Nearly seven years on, however, some of its facets warrant reflection. One notable example are Propositions 3 and 4 (spelled out on p. 39) which are addressed below.

Proposition 3 – Stability could only be attained if the minting technology is weakly convex.

Comment – A weakly convex minting cost implies miners face rising difficulty, potentially smoothing issuance. Bitcoin's difficulty adjustment is convex in energy terms, but its supply cap isn't demand-responsive. The point made in the paper is that stability needs flexibility (optimizing transaction efficiency) akin to medieval mints adjusting coinage when metal flows shifted; convexity mimics this by resisting runaway supply. But there are some nuances to consider, outlined below.

- Bitcoin's volatility stems mostly from speculation, not just supply. Nowadays, 80% of its trade involves futures (leveraged bets). The consequence is that small swings in spot prices trigger margin calls, cascading into more pronounced price changes, which greatly explains the market volatility. Convexity alone won't fix that without linking to demand.
- A convex rule needs coding into a trustless protocol. For example, Ethereum's gas limits approximate this, yet volatility persists. Besides, throughout history stability relied on authority (e.g., the Roman mints).

Rigid minting (Bitcoin's linear halving) amplifies swings, and a convex supply response could dampen them, akin to central bank's smoothing via interventions. Still, who calibrates the rule in a trustless system?

Proposition 4 - Currency competition can only succeed if the issuance of private tokens is bounded.

Comment – Unbounded private money has historically faltered; consider, for example, the over-issuance of notes by U.S. wildcat banks in the 1830s (crashing to the ground during the Panic of 1837). Specie-backed notes (notes bounded to metallic reserves) survived for longer. Bitcoin's 21-million cap mimics this.

This limit on issuance, however, restricts Bitcoin's utility, and explains why it has a low velocity (it hovers at about 1.5, compared to roughly 6 for the US dollar). That's simply because Bitcoin is hoarded, not spent (the speculative HODL culture of expecting gains). Just think about how gold's bounded supply (natural scarcity) led to low velocity in deflationary periods (for example, during 1873–1896 in the UK, when hoarding outpaced spending). Bounded specie held value, yet its velocity lagged when hoarded, limiting its reach.

That said, there were also *hybrid* examples throughout history. Consider, say, the bills of exchange that emerged in Europe in the 1600s as private, negotiable instruments for trade. Issuance wasn't infinite; they tracked trade volume. Bounded by specie, usage grew with economic need (e.g., Amsterdam's bill volume doubled 1650–1700 as trade boomed). They circulated widely among merchants, often endorsed multiple times before redemption (3–5 turnovers in 90 days, implying an annualized velocity of about 4–6). It was a clever way to bridge specie's scarcity with paper's flexibility. Trust came from bounded flexibility, not rigid caps.

In summary, boundedness aids competition by signaling scarcity but success hinges on usability and coordination, where (nowadays) fiat excels. Network effects are key.

Rethinking both Propositions

Considering the above observations, perhaps it would be better to rewrite both propositions as follows:

Updated Proposition 3 – A cryptocurrency is more likely to achieve value stability if its minting process incorporates a weakly convex supply response that adapts to economic demand, rather than adhering to a rigid issuance schedule.

This reformulation bridges convex issuance with demand response, implementable via a decentralized feedback algorithm, while nodding to history's flexible mints.

Updated Proposition 4 – Private cryptocurrencies are better positioned to compete with state-backed currencies if their token issuance is bounded to ensure scarcity, though success also depends on achieving broad acceptance and utility.

It captures the original warning about unbounded issuance while stressing the fact that success isn't just about caps but adoption. Scarcity signals trust, but utility is what seals the deal.

Taken together, then:

- The updated version of Proposition 3 tackles *internal design* – a flexible, convex supply stabilizes value.
- The updated version of Proposition 4 focuses on *external competition* – a bounded issuance aids rivalry with fiat, but acceptance is key.

Seven years later, these tweaks (some of which are mere refinements) align the vision in the original 2018 paper with 2025 realities.

It also explains (and reaffirms the paper's original gist) why Bitcoin thrives as a store of value, not as a currency.