*Cambridge Journal of Economics* 2023, **47**, 535–554
https://doi.org/10.1093/cje/bead008
Advance Access publication 21 April 2023



# Menger or Marx? The political ontology of cryptocurrency

Tully Rector and Jason Grant Allen*,

One of the perennial fault-lines in monetary theory is that between commodity and credit theories of money. The emergence of alternative payment systems based on blockchain and distributed ledger technologies, of which Bitcoin is the most prominent example, has raised a host of important questions in relation to this debate. This article considers two. The first is ontological: Are Bitcoin and similar 'cryptocurrencies' best conceived of as money? The second is political: Do these money candidates represent an emancipatory development over state-backed fiat currency? The ontological question, we will argue, invites the political one. If it is the case, as Chartalists maintain, that (i) for some X to be money it must have certain properties which can only be imparted by political authority (broadly understood) and if (ii) political authority ought to be subject to public control, then attempts by private actors to usurp a social 'money function' cannot count as legitimate political developments. We will argue in support of this position. This discussion is limited to Bitcoin, though its implications generalize for relevantly similar cryptocurrencies. Our method involves considering, first, claims made by Bitcoin's defenders about its status as money, and what accounts for that status. While these claims are often thought to extend Mengerite or generally Austrian lines of economic argument, they resonate more with Marx's theory of monetary value. Moreover, a close assessment of that theory's defects yields specific normative conclusions that potentially undermine the notion that Bitcoin constitutes a valid means of resisting state monetary authority.

*Key words:* Cryptocurrencies, Monetary theory, Value, Austrian economics, Marx
*JEL classifications:* E42, D46l, P48

## 1. Introduction

One of the perennial fault-lines in monetary theory is that between commodity and credit theories of money. The emergence of alternative payment systems based on

Manuscript received 5 January 2021; final version received 2 November 2022
*Address for correspondence:* Jason Grant Allen, SMU Yong Pung How School of Law, 55 Armenian Street, Singapore 179943; email: jgallen@smu.edu.sg
*Utrecht University (TR). Singapore Management University; Cambridge Centre for Alternative Finance, UK (JGA). The authors thank Titus Stahl, Mirjam Müller, Frank Hindricks, and other participants in the Public Philosophy and Social Ontology summer school at Groningen University for their feedback on the ideas in this paper. Thanks also to Armin Zimmermann for insight into the technology and economics of cryptocurrencies. We also thank Rosa Maria Lastra, Michael Kumhof, Simon Gleeson, Saule Omarova, and Will Bateman for discussion and Tony Lawson for comments on the draft. Thanks to Ty Haberland for research support. This article draws on work under Sub-Grant RM02 ('Legal and Economic Conceptions of Money') of UK Economic and Social Research Council Main Grant ES/R00787X/1 ('Rebuilding Macroeconomics') and *Deutsche Forschungsgemeinschaft* Grant Ref. No. GZ: AL 2415/1-1 ('F.A. Mann and his Contribution to the Development of English, German, European, and International Law').

blockchain and distributed ledger technologies, of which Bitcoin[1] is the most prominent example, has raised a host of important questions in relation to this debate. Here we are concerned with two. The first is ontological: are Bitcoin and similar 'cryptocurrencies'[2] best conceived of as *money*? The second is political: do these 'money candidates' represent an emancipatory development over state-backed fiat money?[3] The ontological question, we will argue, invites the political one. If it is the case, as Chartalists maintain, that (i) for some $X$ to be money it must have certain properties which can only be imparted by political authority (broadly understood) and if (ii) political authority ought to be subject to *public* control, then attempts by private actors to usurp a social 'money function' cannot count as legitimate political developments. We will argue in support of this position.

For simplicity's sake, we confine ourselves to a discussion of Bitcoin, though our points generalise for relevantly similar technologies. Our method involves considering, first, claims made by Bitcoin's advocates about its status as money, and what accounts for that status. While these claims are often thought to extend Mengerite (or generally Austrian) lines of economic argument, we think they most closely resemble Marx's theory of monetary value. Moreover, a close assessment of that theory's defects yields specific normative conclusions. These ground a rejection of the view that Bitcoin constitutes a valid means of resisting unjust state authority.

The relevance of crypto-assets for political economy has only intensified in the remarkable period since early 2020, when Bitcoin was priced at around $6,000. Bitcoin was trading a year later at over $60,000, and has since crashed back down to about $30,000. Major firms like Goldman Sachs, UBS, and BlackRock—the world's biggest asset manager—which had previously shown little interest in crypto-assets, have in this period rushed to develop stakes in the new asset class. In April 2022, Rishi Sunak, then UK Chancellor of the Exchequer, stated his 'ambition to make the UK a global hub for cryptoasset technology', announcing a suite of measures to 'to ensure the UK financial services sector remains at the cutting edge' of the crypto market (HM Treasury, 2022). While some economists are sanguine about the effects of this market's radical expansion, others see close analogues with previous financial manias and warn of a potentially drastic implosion, even comparing it unfavourably to Madoff-style Ponzi schemes (Quinn and Turner, 2020; McCauley, 2021). The recent implosion of the Terra/Luna 'stablecoin' system has brought the darker side of the crytoasset-based financial economy into stark relief (Faux and Shen, 2022). Although so-called stablecoins are a distinct asset class to Bitcoin, the incident has also showed how connected the prices of different crypto-assets (including Bitcoin) are. Questions about the nature, form, and source of Bitcoin's value have led to suspicions that this value obtains *solely* by virtue of an owner being able to sell it to a 'greater fool' (Kjærland *et al.*, 2018).

[1] We follow the convention of using Bitcoin (capitalised) to refer to the network and Bitcoin (lower case) to refer to the unit or asset, for example: 'One Bitcoin represents 1/21,000,000th of the unspent transaction output (UTXO) on the Bitcoin blockchain' (Nakamoto, 2008).

[2] The term is widespread but begs the question of 'currency' and therefore 'money' status. In many contexts, it is safer to speak of 'cryptoassets'. We take a cryptoasset to be an instantiated data object, that is a packet of digital data, that is ascribed market value in virtue of the socio-technical features of the network in which it is created and used. These features include a cryptographic security layer, some economic incentive design layer, and typically some kind of distributed but rigid governance layer. A cryptoasset may be used as a currency (as any other asset may be) in certain contexts and circumstances (Allen *et al.*, 2020).

[3] We understand 'fiat' money to be an imprecise but useful term that denotes money (i) issued by, or with the authorisation, of a public authority and (ii) issued without any reserve of assets backing its value.

The growth in the cryptoasset market has also led to widespread concern over the climate impact of digital mining. The kwH needed to verify transactions rivals the total energy consumption of entire nations.[4] There have recently been serious discussions, at the level of the European Union and the Swiss Federation, to ban cryptoasset protocols like Bitcoin that use a 'proof of work' (PoW) consensus mechanism (Szalay, 2022).[5] Broad dissatisfaction with PoW has motivated the development of blockchain protocols that use some other model of transaction validation, such as 'proof of stake' and 'proof of authority'.[6] The leading platform for blockchain-based financial innovation, Ethereum, has moved away from the PoW model.

Our argument in this paper is that these debates and developments are not just incidental to the core question of Bitcoin's value. They relate to the way that a transaction (i.e. a transfer of value from one user of the system to another) is validated to avoid the central problem of any digital information-based value transfer system: the fact that digital data can be duplicated at close to zero marginal cost, and are not *per se* rivalrous or excludable. The way that a record-keeping system solves these problems (i.e. through a central intermediary such as a bank or through a decentralised system of 'trustless' validation, such as a blockchain data structure) inform that system's bid for the status of a 'monetary' system. All such systems involve both technical and social or governance layers. Such considerations motivate a deeper study of the ontological structure of blockchain-based money candidates, and the social and political implications of that structure's defining features. Our paper is a contribution to that effort.

Section 1 presents the relevant background for understanding (i) how ontological questions bear upon political economy generally, and (ii) Marx's monetary thought in particular. Section 2 develops the standard account of Bitcoin's value in terms that disclose its overriding (or underlying) debt to Marx. Section 3 mounts a Chartalist critique of Bitcoin. The Conclusion summarises our overall argument and suggests some further directions for research.

## 2. Marx on money

Stated at its broadest, a social formation accounts for the allocation of economic outputs across its membership by advancing paired claims of desert and necessity. In ours, desert is typically defined in contributive terms: those whose labour or capital inputs add more value to the goods produced merit a proportionally higher share in or access to valuable goods (Mazzucato, 2019). Since that reward, we are told, is what generates the disposition to create value, everyone is better off—has optimal access to value—only when our institutions deliver it. Defenders and critics of those institutions alike thus cannot avoid the question of *what constitutes and measures value*, and hence the

[4] See e.g., the Cambridge Bitcoin Electricity Consumption Index (Cambridge Centre for Alternative Finance, 2023)

[5] The proposed Markets in Crypto-assets Regulation in EU law originally contained a provision prohibiting proof-of-work from being 'environmentally unstable'. This clause was removed in March 2022.

[6] Proof-of-stake is an alternative built-in consensus mechanism used by cryptocurrency networks. People operate as 'validators' in order to keep the network secure. End-users are rewarded with cryptocurrency for validating transactions, by 'staking' their coins on the network in return (typically) for transaction fees. Another recently popular alternative is the proof-of-authority consensus method, where blocks are similarly validated by a select group of accounts. The automated process provides this limited number of actors to update the blockchain more frequently and with lower transaction fees. Both mechanisms operate at a significantly lower energy consumption than proof-of-work.

question of money, insofar as money both represents and embodies economic worth. Legal authorities must decide not only who has which claim to what goods (including the state's claim to wealth held by individuals), but also what counts as a valid medium in which any such claim can be settled. This leads to the ultimate question: *who can create that medium*. As money is not a natural kind but a 'social construction', the power to shape that construction, and the effects and entailments of this power being used in one way rather than another, are problems at the intersection of political economy and social ontology.

All political programs that have sought basic changes to the *money form*—as opposed to its patterned distribution—have employed socio-ontological arguments. For example, Proudhon and the Ricardian socialists, in blaming the medium of exchange for the miseries of production, claimed that only money which embodied the labour responsible for a commodity's real value (so-called *labour money* or *time chits*), not gold or silver, could put market relations into moral and rational equilibrium. Debates within the early socialist movement turned on these kinds of questions. While Marx also held a labour theory of value, he viewed Proudhon's efforts to 'republicanize specie' as a political mistake reflecting metaphysical confusion over money's basic nature and attributes (Proudhon, 2011; Roberts, 2018).

Critics of contemporary capitalism have taken a more Proudhonist line, endorsing formal innovations that make use of money's digital character. According to David Harvey, for example:

> "While the utopian aim of a social order without exchange value and therefore moneyless needs to be articulated, the intermediate step of designing quasi-money forms that facilitate exchange but inhibit the private accumulation of social wealth and power becomes imperative."(Harvey, 2014, p. 35)

Harvey suggests delinking money's *circulatory function* from its *value-storage function*, by engineering its digital structure to dissolve if unused after a set time period.[7] From a different point on the ideological spectrum, anarcho-libertarians have defended the use of cryptocurrencies (such as Bitcoin) as a way of evading domination by centralised authority. States and large financial institutions, on this view, possess unwarranted power to issue money, manage its supply, monitor its use, and extract rent from its storage and exchange—practices that infringe the natural contract, property, and privacy rights of autonomous individuals.

Considering the merits of such a claim requires an adequate grasp and appraisal of the ontology, explicit and implicit, on which they rely. That ontology specifies the type and range of properties an entity must have in order to be designated by the concept of money, and what has to be the case, in the social world, for an entity to take on or exhibit those properties. Debates over the ontology of money, then, can be framed as debates over the concept's *intensional content* and *extensional scope*.

We focus here on the ontology implied in the standard arguments for Bitcoin. Despite their libertarian origins, our argument is that they rely on an essentially Marxist conception of the money form. That conception, and the space in which it confronts rival versions, has once again become the subject of some scholarly debate, not least in

[7] An idea first proposed by Silvio Gesell, and briefly implemented via time-stamp currencies in parts of Austria and Germany during the Great Depression (Keynes, 2016). That governments might use similar mechanisms to escape the lower-bound on interest rates has also been recently suggested (Assenmacher and Krogstrup, 2018).

this journal. Ingham, for example, has positioned Marx alongside the Austrians as a 'substance' theorist, for whom the value of money resides originally in some entity or process whose value exists prior to being rendered into a distinctly monetary unit of account (Ingham, 2018). Weber, by contrast, emphasises what she takes to be crucial differences between Marx and the Ricardian and neoclassical theorists, differences which have little to do with a 'substance' ontology (Weber, 2019). Marx's main insight, on her view, was to identify money's 'universal' and 'synthesizing' value in terms of its being a 'general commodity'. Suitably clarified, these insights are said to buttress contemporary theories of money, like Lawson's, which focus on the features according to which social decisions 'position' some entity *as* money (Lawson, 2018).

The fact that debate over Marx's considered views of money remains intense—and, hence, that the application of his views to today's cutting-edge monetary dynamics remains a delicate and rather fraught enterprise—stems in part from the obscurity with which Marx presents his conception in *Capital*. The remainder of this section will delineate what we take to be the most general features of that conception. These will later be mapped on to the claims made about cryptocurrencies by their representative advocates.

We take Marx's mature position on money to be set forth in *Capital*, especially the first volume, which begins with an analysis of money as a type of value shared by all commodities. Reconstructing the ontology requires that we state briefly what 'value' means in that analysis. For Marx, a commodity had three dimensions of value—*use-value*, *exchange-value*, and *value*. The first denotes the correspondence of a commodity's properties to some human aim or need; the second denotes the ratio at which bearers of use-values correspond to one another in market exchange; the third denotes that by virtue of which all commodities are commensurable, namely what Marx calls *socially necessary labour time*, defined as 'the labour-time required to produce any use-value under the conditions of production normal for a given society and with the average degree of skill and intensity of labour prevalent in that society' (Marx, 1982, p. 129).

Marx inherits much of Ricardo's schema, adding the crucial determining element of *social necessity*, which both historicises and politicises the process of value-creation. In any case, the three values interanimate the commodity, and none can be understood without reference to the others. The last, however, has ontological primacy: it is the labour inputs that all commodities contain which accounts for their being exchangeable *as* equivalent relata. But on the plane of exchange, the labour in question is purely abstract, and the value it imparts is intangible. Thus, the practice of exchanging equivalents at scale logically requires a means by which value can show up as a magnitude for transacting parties. The bearer of *that* magnitude would then be the *general* equivalent: that one commodity whose exclusive use-value *just is* its exchangeability for any other commodity. *Capital* develops, then, a commodity theory of money.

Marx develops out of the above points a rococo theory of equilibrium pricing whose details need not detain us. The important initial takeaway is that for any $X$ to be a measure of value *for* commodities, it must have the sort of properties that make something valuable *as* a commodity, and an $X$ has those properties if and only if it encodes some magnitude of socially necessary labour time. Here we see why Marx disagreed with other radicals about monetary reform. The reduction of all labour value to one homogenising general equivalent, and the conferral of labour's value in terms of that equivalent: this what the early socialists identified as the operation of capitalism's alien, coercive power, which confined an entire class of producers to degradation and

poverty. While Proudhon and the Owenites ascribed these effects to the medium of exchange, Marx rooted them in the practice of commodity production as such, which bound every product of labour (and hence *all labour*) to a single value-conferring *telos*: the exchange transaction. Money's nature as a measure of value, then, is already conjured in, and by, the commodity form. Money-based 'transaction' renders the labour that produced the commodity *offered* equivalent to that which produced the commodity *received*—it takes its measure, as it were. This explains Marx's famously gnomic proposition: 'all commodities are perishable money, but money is the imperishable commodity' (Marx, 1993, p. 149). The exchange relation both determines, and is determined by, the value structure according to which commodities appear as measurable (and commensurable) entities. In short, we cannot isolate money's economic role from its codetermining social facts.

For Marx, money's various roles—store of value, medium of exchange, fungible debt/credit instrument—do not define its ontology, but follow from it. Money is a social relation, to be sure, but on account of its indurating the labour responsible for value. That is what enables it to measure value, and thus to denominate any commercial credit and debt relation. Marx, of course, assumed a metallist monetary standard, and there is much cerebration in *Capital* over links between the amount of labour inputs required for gold production and the variability of prices in equilibrium. The state's role here, and overall, is merely to standardise in coinage the quantities of the money commodity, enforce the representational utility of banknotes, and so on. State-issued fiat money's disconnection from originary labour processes, and its susceptibility to inflationary pressure, made it a superficial epiphenomenon for Marx (Itoh and Lapavitsas, 1999). This is in keeping with his general view of state authority as belonging more to the 'superstructure' than the 'social base'.[8] The state essentially comprises techniques of domination secreted by capitalist property relations—in the *Manifesto*'s famous dismissal, 'a committee for managing the affairs of the whole bourgeoisie' (Marx and Engels, 2017, p. 10). Others have argued that Marx made room for a more autonomously extractive, though still adjutant-like, capitalist state; either way, *the state is not basic to Marx's view of the ontology of money*. This is a function of its being programmed, as it were, by primary market dynamics. Marx could not be further in this regard from the Chartalists.

We can now isolate the core elements of Marx's ontology of money. Its credit and liquidity functions require the existence of properties (whatever these turn out to be) to which value can be attached. The value-storage function, in turn, requires that those properties be modally robust, or present across the widest possible range of exchange conditions. Their capacity to measure value is the proof, as it were, of their being so. For such properties to serve the ontologically primary function of measuring value, the bearer of those properties, whether gold or silver or something else entirely, *can only come into being as a value-bearing kind through some process of human work*. It is labour that accounts for value being attached to the properties that carry it, not an authoritatively symbolic act or declaration. Undistorted manifestation of value—a condition of equilibrium—depends on some public, shareable manifestation of the labour responsible for money's existence.

[8] The first comprises those non-economic institutions, largely legal and political, whose characteristic properties are explained by reference to a subtending economically productive system (the 'base'). The superstructure's function is to facilitate and promote the economic relations favoured by the productive forces (Cohen, 2020).

## 3. Accounting for the value of Bitcoin

As we have seen, questions about the social ontology of money and its place in political economy often have a practical aspect. Today, that aspect is given by the cryptocurrency movement that has arisen in the past decade. Bitcoin was presented in 2009 as a private money system. Technical limitations, in particular its transaction validation process speed and cost, make Bitcoin quite ill-suited to performing certain functions of money; its empirical patterns of use point to it being a speculative asset, rather than a medium of exchange or even a store of value (Yermack, 2013). Outside of a rather niche community, *quanta* of Bitcoin are generally priced in fiat currencies and 'BTC' is seldom used as a general unit of account. But we will take the claim at face value, asking how Bitcoin enthusiasts should present their claims about the value of Bitcoin, and what Bitcoin might tell us about the relative merits of different approaches to money.

There is a decidedly 'Austrian' element within the cryptocurrency movement (Weber, 2016). Austrian Economists and Bitcoin enthusiasts share common cause in (i) a critical view of central banking and reserve fractional banking, (ii) a preference for free banking, monetary competition, and commodity-based money, and (iii) a broadly libertarian outlook that favours spontaneous individual action over collective political choice procedures. And yet, the feeling is not always mutual. One rather exasperated op-ed in *Bitcoin Magazine* from 2014, for example, reported that someone attending a Bitcoin conference in that year would be 'shocked at the widespread acceptance of Austrian Economics among Bitcoin enthusiasts', but complained that the majority of Austrian Economists not only failed to appreciate Bitcoin and cryptocurrency but were 'very critical' (Best, 2014). As such, there has been a debate about whether and how (i) Austrian Economics might be applied to prove Bitcoin's case for money status and (ii) Bitcoin might provide a case to test the adequacy of Austrian theory (Hansen, 2019). The desire for an 'Austrian' explanation for Bitcoin, however, seems to be born of a sectarian desire for coherence rather than natural fit. In our view, Bitcoin should be explained in Marxist terms by its advocates.

Austrian Economists posit a 'catallactic' theory of money: they approach the value of money as a matter arising from individual choices made by market participants. Carl Menger worked from the premise of the double coincidence of wants in (what he terms) 'primitive' societies, in which 'each man is intent to get by way of exchange just such goods as he directly needs, and to reject those of which he has no need at all, or with which he is already sufficiently provided' (Menger, 1892, p. 242) On this view, it is not the *use-value* of a commodity, nor the *labour* invested in its production, that determines its value; a commodity's value *is* whatever a market participant is willing to pay for it, which derives from her calculation of the commodity's (i) scarcity and (ii) marginal utility (Menger, 1871, p. 77 *et seq*).

Menger conceived of utility in terms of the ever-fluctuating, essentially contingent, subjective desires and preferences held by consumers, and insisted that this sort of utility was the prime locus and *explanans* of economic value. Preference-strength imparts that value to goods, and transitively to the labour and inputs involved in the goods' production. It is convenient to contrast this with Marx's view set out in the section above. The Marxian idea of use-value refers to the comportment between a good's objective features and the human needs it can satisfy (in virtue of having those features). The point for Marx was *contrastive*: under capitalism, exchange relations are

governed by a universal equivalent (i.e. money) in terms of which any given commodity is compared to any other. 'Exchange value' is defined by its abstraction from the real properties that make goods useful. The problem, for Marx, in having money be the comparability structure in which economic value becomes determinate—the problem with *exchange-value trumping use-value*—is that it obscures the actual process that creates worth, which is labour. Labour causes goods to have the features that make them useful. Goods, therefore, are rightly understood as definite magnitudes of crystallised labour-time. Menger, a pioneer marginalist, flatly rejected this. *That* a commodity had any utility was wholly evidenced by a consumer's willingness to part with something in order to acquire it, so the measure of that utility was, in turn, given jointly by the thing he was willing to part with, and the extent of his willingness. There was no need, for Menger, to privilege labour: labour created the *goods* but not their *utility*.

For Menger, a commodity attains monetary status in virtue of its 'saleability' relative to other commodities. The Austrian approach to money thus rests on a 'regression theorem', which is also developed in the work of Ludwig von Mises. According to Mises, once certain basic conditions are met (namely, the division of labour and tradeable private property rights) individuals begin the process that eventually results in the adoption of a marketable commodity as money. The value of a commodity as a medium of exchange, however, presupposes a pre-existing 'objective' exchange-value that arises from market demand *based on its use-value*.[9] Murray Rothbard explains:

> Demand for a good as a medium of exchange must be predicated on a previously existing array of prices in terms of other goods. A medium of exchange can therefore originate only… out of a commodity previously used directly in a barter situation… Money must develop out of a commodity with a previously existing purchasing power, such as gold and silver had. It cannot be created out of thin air by any sudden "social compact" or edict of government (Rothbard, 2009).

In other words, the regression theorem demands, or presupposes, a commodity with certain properties, including *some* use-value logically prior to its exchange-value. This conjectural history of money has been criticised as being falsified by the actual historical record by Ingham, in particular (Ingham, 2004; North, 2012). However, we are not concerned with a substantive critique in this paper.

There are well-founded questions about Bitcoin's ability to satisfy the regression theorem. Bitcoin appears more like a private, hyper-fiat currency than anything else. *Quanta* of unspent transaction output on the Bitcoin blockchain have no 'intrinsic' value and certainly no use-value as such; they were created from 'thin air' and are useful *only* because they can be used as a 'token' of value. Of course, 'Austrian' Bitcoin enthusiasts will argue that *quanta* of unspent transaction output, as immaterial goods, can and do conform to the regression theorem. It is surely correct that immaterial objects can serve as the medium of exchange between economic actors. But the important question for our present purposes is: What are the properties of Bitcoins, as *technological artefacts*, that make them capable of functioning in this way? What is it that makes a Bitcoin 'saleable', or in any way functional as an 'object' that can represent exchange-value? The answer to those questions will differ based on a granular analysis of the relevant object in question, and here we are concerned with 'Bitcoins' specifically. In our view, the properties of the Bitcoin network *qua* socio-technical system are not, in fact, well described in Austrian terms at all.

[9] See Hansen (2019).

The crucial aspect of Bitcoin's money candidacy is the *consensus mechanism* by which transactions on the protocol are validated and by which individual Bitcoins are kept scarce. Bitcoins are informational units—'electronic signatures' in an interlocking 'chain' of such signatures[10]—that could, in theory, be replicated *ad infinitum*. Unlike in a physical token system (such as cash, where unique *physical* tokens represent units of value) digital information can be replicated without significant cost or degradation. If its reproduction is unrestricted, a 'chain of digital signatures' is inutile as a token of a unit of value, because of the so-called double-spend problem: 'the payee can't verify that one of the owners did not double-spend the coin' (Nakamoto, 2008). As the Nakamoto Whitepaper explains, the usual solution to this problem is centralised record-keeping by a trusted third-party, such as a bank. The purpose of the Bitcoin protocol is to enable bits of information to function as tokens of units of value without recourse to such an agency.

This is achieved by means of a consensus mechanism which relies on PoW. PoW was apparently first proposed for discouraging spam email in 1992 (Dwork and Naor, 2001). That proposal effectively imposed a *computational cost* on sending an email, such that spammers would have to weigh the cost of sending large numbers of unsolicited emails against the anticipated benefit of doing so (e.g. for advertising).

The direct antecedent of Bitcoin cited in the Nakamoto Whitepaper was the 'Hashcash' system, proposed as a means to 'throttle systematic abuse of un-metered internet resources' such as email in 1997 (Back, 1997).[11] Probably a result of parallel development, the idea is essentially the same; building on Chaumian cryptography, Hashcash involves the addition of a Hashcash stamp in the header of an email, which imposes a computational cost on using the protocol. In this way, the contents of an email—bits of information—can be made artificially 'scarce' and can therefore be treated as representing a quantum of value. A 1999 paper defines the notion of a proof-of-work as 'a protocol in which a prover demonstrates to a verifier that she has expended a certain level of computational effort in a specified interval of time'; in an 'implicit' PoW protocol, verification is not performed by a verifying party as such, but by 'the ability of the prover to perform a given task' within the network (Jakobsson and Juels, 1999, p. 264).

What does the role of a PoW consensus mechanism entail for the value proposition behind Bitcoin? In our view, it is highly significant: it changes the value proposition from one based on the *market choices* of individuals engaged in commodity exchange, to one based on the *necessary labour time* invested in verifying the validity of the 'electronic coin'.

Just prior to the launch of Bitcoin, Nick Szabo published a proposal for a system called 'bit gold' (Szabo, 2008). Bit gold has not been operationalised, so it is of interest mainly as an historical stage of Bitcoin. Szabo's (2008) proposal for bit gold was based on computing a string of bits from a string of challenge bits using a PoW function.

[10] See Nakamoto (2008).

[11] Hashcash is distinct from HashCash, which is a particular digital payments system. As an aside, true cash systems use *physical* tokens that are transferred by changing *physical* possession. It is this transfer of physical possession of moveable tangible property that the legal system treats as a change of ownership. There is currently no established legal regime for the existence of cryptographic tokens as objects of property rights, and, assuming property rights in such objects exist, the method for transferring those rights is not clear. In our view, analogies to cash are a poor place to start and exhibit a naïve ontology that is based on heuristic shortcuts in reasoning rather than serious engagement with the ontological nature of digital payment systems (Allen, 2019a).

'The resulting string of bits is the proof of work' (Szabo, 2008). Precious metals and collectibles, he argued, have an 'unforgeable scarcity due to the costliness of their creation', and it is this costliness that allowed commodity-based monetary systems to operate without a trusted third-party. However, metallic money systems suffered from security problems (coins could be stolen) and assaying the metals used in transactions was costly, leading to dependence on trusted third parties (e.g. mints) to verify the metallic content of the coins. 'Thus, it would be very nice if there were a protocol whereby unforgeably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust' (Szabo, 2008).

At the time, a version of this had been operationalised by Hal Finney called 'Reusable Proof of Work' or RPoW. *Cryptowiki*, an online encyclopaedia of cryptography, explains that Finney's RPoW system was used as 'token money':

> Just as a gold coin's value is thought to be underpinned by the value of the raw gold needed to make it, the value of an RPoW token is guaranteed by the value of the real-world resources required to 'mint' a PoW token (Anon., 2023).

RPoW is also a Hashcash-based system, but relies on certain hardware features which are theoretically capable of subversion. Bitcoin, on the other hand, uses a purely computational mechanism to solve the double-spend problem. Using PoW, a payee can know with a high degree of probabilistic certainty that the previous owners did not sign earlier transactions by reference to a public ledger, visible to all participants in the system, and can agree on a single history of transactions in that shared ledger.

In our view, *this* is what must support Bitcoin's apparent capacity to function as money. While the cryptographic protocol represents an advance on the bit gold proposal, the broad features of the system are much the same. Bitcoin thus solves the double-spend problem by cryptographic means, which in turn rest on game-theoretical presumptions about incentives and participants' motivations[12]:

> Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, *which has the greatest proof-of-work effort invested in it.* If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, *an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes…* [T]he probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added (Bitcoin Wiki, 2023).

Again, scarcity makes Bitcoins money candidates, and that scarcity derives from the application of computer processing power. Indeed, the importance of the work embodied in each 'coin' is suggested by the metaphors of 'minting' and 'mining' for adding transaction records to the public ledger of past transactions. As one Bitcoin wiki explains:

[12] Because the first transaction in a given block creates a coin owned by the creator of the block, i.e., the one who has performed the work required for the verification process, an incentive is created 'for the [verifying] nodes to support the network' and puts new 'coins' into circulation without a central 'mint'. Thus, it is assumed that even if a 'greedy attacker' were to command the amount of computational power in the network sufficient to subvert the proof-of-work consensus mechanism, 'he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins'. Nakamoto assumes that the attacker is economically rational, such that 'he ought to find it more profitable to play by the rules' as he rules 'favour him with more new coins than everyone else combined' rather than 'undermine the system and the validity of his own wealth' (Nakamoto, 2008).

> Mining is intentionally designed to be resource-intensive and difficult so that the number of blocks found each day by miners remains steady. Individual blocks must contain a proof of work to be considered valid. This proof of work is verified by other Bitcoin nodes each time they receive a block… The primary purpose of mining is to set the history of transactions in a way that is computationally impractical to modify by any one entity (Bitcoin Mining, 2023).

One website promoting Bitcoin mining claims that PoW is a method to ensure that new blocks are costly to make; mining costs processing power, which equates to (i) hardware, (ii) energy, and (iii) time. The provider of one of the early Bitcoin to fiat exchange services described his method of calculating the price of Bitcoins in the following terms:

> The exchange rate is the average of the adjusted Bitcoin production per day divided by the average *production costs per day*… Production costs consist of the price of broadband Internet and metered electricity… During 2009 my exchange rate was calculated by dividing $1.00 by the average amount of electricity required to run a computer with high CPU for a year, 1331.5 kWh, multiplied by the average residential cost of electricity in the United States for the previous year, $0.1136, divided by 12 months divided by the number of Bitcoins generated by my computer over the past 30 days (New Liberty Standard, 2023).

In other words, validation establishes the value-bearing properties of the informational unit in question, which is cast as an 'electronic coin' *because and only to the extent that* it requires the investment of time and computing power. Currently, the incentive for those processing transactions is a combination of fees per transaction and a competition with other validators for new 'Bitcoins' in the system. According to the design of the system, the latter will gradually phase out to yield a fee-only based system. This is not material to the central point: it is only the socially necessary labour time invested in the validation of a Bitcoin transaction that makes it the case that market participants can treat unspent transaction output on the Bitcoin blockchain as a representation of units of value at all. This is logically prior to any question of 'saleability' in the Austrian schema: we are talking about the properties that make 'Bitcoin' saleable rather than worthless bits of data sitting in some digital database. If these circumstances did not obtain, that database could not be used as a probabilistic proof-of-value ownership at any given point in time.

On this basis, we think the Nakamoto proposal is most straightforwardly described as one based on a Marxian theory of value. Incidentally, one virtue of this approach—however accidental—is to ground Bitcoin in the physical economy necessary to create and sustain the Bitcoin system. One might intuitively think that, because something is digital, it is in the 'ether'. But Bitcoin has a physical footprint: 'mining rigs' occupy physical space, consume electricity, create waste heat and noise (and carbon emissions), and require human maintenance (Stoll *et al.*, 2019). Again, these things are not just incidental: *they are the reasons that Bitcoin unspent transaction outputs are scarce*. If we lived on a world where the capital necessary to validate Bitcoin transactions were infinite, the whole game-theoretical premise of the mining system would break down. At the end of the day, to the extent that Bitcoin can be 'commodities' at the base of an Austrian regression, it is because each unit of unspent transaction output on the Bitcoin blockchain represents the *investment of socially necessary labour time*.[13]

[13] We observe that not all present inheritors of Marx share the labour-theoretic position *vis-à-vis* Bitcoin that we critique in this paper. Rotta and Paraná (2022, p. 6), for example, argue in a recent paper that very little 'socially necessary direct (living) labour' is invested in in mining and verification processes, which ought rather to be seen as transfers of value: Bitcoin is, on this view, a 'digital commodity' but not a monetary form.

The Austrian view of money was advanced in the late 19th century, not only against then-current labour theories of money but also against the Chartalist view that money was a creature of the state. In other words, where the Chartalists saw an exercise of public authority as something implicit within the ontology of money, Menger thought that the existence and properties of money could be explained by reference to spontaneous economic transaction alone. 'Money', argues Menger, 'has not been generated by law. In its origin it is a social, and not a state-institution. Sanction by the authority of the state is a notion alien to it' (Menger, 1892, p. 255). This probably explains the *prima facie* attraction of the Austrian School for advocates of Bitcoin. However, in our view it reflects neither the logic of value to which they appeal in their defence of Bitcoin, nor the political logic of money in a broader sense.

## 4. A Chartalist critique of Bitcoin

In the discussion immediately above, we argued that the real ontology of Bitcoin is quite different to what most partisans of Bitcoin say it is. Presenting a Marxian theory of Bitcoin's bid for monetary status also provides a context to evaluate the adequacy of Marx's social ontology of money. In this section, we turn to a critique of commodity theories of money with the aim of (i) tracing the borders of a more nuanced treatment of Bitcoin's bid for money status and (ii) using the 'hard case' of Bitcoin to advance our general understanding of money and value. Both Marx and the Austrians are commodity theorists, and metallists specifically. We think their accounts are equally vulnerable the same basic critique. We will focus on Marx, however, as it is more illuminating for the case of Bitcoin, given the constitutive role that PoW plays in it.

It is not obvious that distributed ledger 'currencies' represent an historical change in monetary form, still less a mutation in money itself (Lawson, 2019). As a type conceived not as a set but as a kind, money has always, by definition, been abstract, however concrete its tokens (be they stone, cowrie, metal, paper, or digital); the dematerialisation of those tokens has anyway been accelerating for decades, as rapidly as technological means have allowed. That Bitcoin represents a new monetary *institution* might seem more plausible. Money has been called 'the oldest public–private partnership': entrepreneurs devise credit instruments to lower their transaction costs, creating new allocative flows for financiers to administer, when and because governments use their authority to standardise such instruments in, or as, a general equivalent (Streeck, 2018). That authority supports, in turn, the powers enabled by tax revenue and debt finance. Bitcoin's ideological partisans seek generally to constrain or contest state authority by appropriating that power. A distributed digital apparatus is said to be more democratic, both operationally and expressively, than a central bank, and by having all transactions accessible to all users, it helps temper the disequilibriating effects of informational loss. These hopes depend on Bitcoin having the value-bearing properties ascribed to it. As we have seen, something like Marx's labour theory of value underwrites those ascriptions implicitly.

Of the many questions raised by our account, two are conspicuously important. The first is ontological, the second normative. The ontological question is: does the labour-theoretic explanation establish that Bitcoin is *money*, as opposed to something like a bill of sale or a collateralised debt obligation whose value depends on its *convertibility into money* (Pistor, 2019) That problem is distinct from, but related to, the normative one: what good would be promoted by replacing fiat currencies with Bitcoin? We address these questions in turn.

Marx's ontology of money does not obviously stand or fall with the labour theory of value, considered as a model of equilibrium pricing. About the latter, economists almost uniformly agree that it fails. Labour is only one productive input, and it is highly diverse; its deployment costs must therefore depend sensitively on conditions affected by demand. Whether Marx intended to explain market pricing in that way is somewhat controversial, and can be passed over here. The point, for Marx, is that a general value metric comes into being with production for the market, and the medium on whose properties that value supervenes will have behind it, in its causal history, some amount, character and duration of human work. This work's social necessity just *is* the value its output encodes. Marx's view succeeds, we submit, in one respect: *it locates money both within and outside the catallactic boundary*. That is, the *need* for money is shown to arise precisely when commodity production is undertaken, as one of its immanent conditions. Only a process *external* to the mutual adjustments of exchange, however, can satisfy that need. Marx identifies that process as socially necessary labour, where the modifiers reflect the reliance of market exchange on a set of relations that are not themselves the outcome of market actors' mutual adjustments. This is one thing we mean by the market's 'social embeddedness' (Cunningham, 2005).

But Marx goes wrong in two ways, in our view. First, he thinks that those adjustments must be mediated by *another* commodity, something that shares the self-same value form with the things whose value it measures. Like all metallists, Marx assumes the function of money can only be served by an entity that has value antecedent to its playing that role. Secondly, he defines this ontologically primary value form in terms of the labour behind it. Bitcoin's defenders perpetrate the second error, if not exactly the first, and lose the merit we identified above. That is, they attempt to position money entirely *inside catallaxy*, as an instrument of order emerging from the practical requirements of private commerce. Those conditions create, as it were, utility gaps. *The work involved in creating a product to fill those gaps establishes the value inherent in that very product.*

Whatever is responsible for the properties that make something useful account for the fact that it has a position in the circuit of commerce, *pace* Marx. But this reduces 'use-value' to a single principle of commensurability. While any commodity can be assumed to have properties that are valued because they serve some need or aim, not everything with use-value is a commodity. Friendship, for example, is valuable on account of the human desire for intimacy, social flourishing, mutual support, and so on, but to commodify a friendship—to offer it for sale—is to abolish its value. Money in its token occurrences can have the use-values appropriate for commodification, so the claims of the commodity theorist, when true, will quantify over *exchanges*: Forex arbitrage, swapping USD for JP¥ at Narita airport, and so on. When you buy an ancient Mysian *stater* at the rare coins auction, you also make the commodity theory true, despite the *stater* no longer functioning as a general equivalent or unit of account. That it once did so, and was crafted for that end, explains both the particularity of its features—being made of electrum, with a griffin and tunny fish on one side and an incuse square on the other—and the value attaching to those features, as expressed by the bidder's offer. If the object had exactly those physical attributes, but were instead an ancient piece of jewellery fashioned by an artisan rather than a *stater* minted by the city-state of Kyzikos, it would satisfy a different need, and have a different value. Money can be a commodity, therefore, insofar as its concrete token occurrences have use-values that furnish us with reasons to transact. But those values specific to money's token occurrences rely on the *kind* being something other than a 'commodity'.

In his classic defense of the credit theory, Innes pointed out how the range of commercial needs on which commodity theorists base their ontology of money could be met by a multitude of individual promissory obligations alone (Innes, 2004). It is no accident that Innes' sophisticated account followed the 18th and 19th century explosion of 'negotiable instruments' law by which immaterial creditor–debtor relationships were 'wrapped in paper' and handled as if they were things (Allen, 2019b).

The prospect of default on a claim, of course, requires shared agreement among transacting parties on what would count as adequate restitution, when the promised good cannot be itself the measure. There needs to be a general unit of account. Importantly, no individual party can settle what that unit is, however, without disadvantaging other parties; since it is in the general interest of all transacting parties that some settlement be made, each has sufficient reason to accept a common authority's settlement. So, while the need for a single unit arises in and from market exchange, it cannot be satisfied by processes of market bargaining alone. Only a *normative* actor *outside* the market can decide on behalf of the general interest.

This discussion touches on the debate about how 'emergent social entities' such as money arise, and what the 'thing' that is (or is treated as) money actually *is*. Time precludes us from going into detail on that debate here. For our present purposes, it suffices to note that Lawson has argued convincingly that the apparent cleavage point between 'commodity' and 'claim' theories of money is more illusory than real.[14] In fact, both commodities and claims require some superadded process (which Lawson describes as 'positioning') *in order to function as money*. This process occurs, and can only occur, within a social constellation. On both Lawson's view, it is this 'positioning' that is most crucial to the understanding of money, along with all other 'social stuff'. Cast in Lawson's terms, then, our question is: what kind of normative actor outside the market can authoritatively appoint a certain thing to be, or act as, the kind of general unit we are concerned with?

In our view, that actor is the state, broadly defined. It is important to emphasise here that by 'state' we don't mean *only* the Weberian apparatus or Westphalian nation-state form, but *any* locus of public political authority. In other words, *state*, in our account, contrasts with *market*—not with band, tribe, empire, or the various offices and bearers of authority responsible for taking political decisions within those structures. That *states* historically set the unit of (credit) account in terms of some already existing commodity does not mean that the commodity's pre-monetary value explains the value it attains upon becoming the common measure, the general equivalent. Nor does it make any general equivalent *ipso facto* a commodity. Rather, any credit device is valued as money when and because market actors believe—and believe that their possible and actual counterparties believe—that the device can be redeemed for commodities of any kind.

*Whatever makes those beliefs true, makes it the case that something is money.* The central question, then, is: what grounds those beliefs? Alexander Douglas (2015, p. 90) puts the question this way:

> If money is just an IOU, then there should be as many types of money as there are debtors… (but) how do we go from a society in which no single type of item dominates others as the medium of exchange, into our own, where currency (or bank deposits guaranteed to be convertible into currency at par) is that item?

[14] In particular, there has been a fruitful debate between Tony Lawson and John Searle on the nature of social objects such as money and how 'money' relates its tokens (Lawson, 2016, 2018).

Douglas' question is not just an historical question, but an ontological one. According to the Chartalist theory of money, the fact that every market actor is indebted to a single creditor makes that creditor's promissory obligations become a universally fungible credit instrument; in other words, you will accept what you know will always be taken *by* everyone else as a means of payment, since it is demanded *of* everyone by a common creditor. According to the classical reading of the 'state theory', the singularity of that creditor resides in its capacity to impose a debt burden—taxes—which no private market actor, by definition, can do: only an authoritative, legitimate apparatus of public power can extract tax revenue, thereby creating, in addition to the public goods for which that revenue is earmarked, the unit of account by which all goods public and private can be valued. While the classical state theory perhaps stresses the importance of taxation too much—one could imagine a non-taxing state with a functioning monetary system—it is beyond doubt that taxation has played an important historical role in almost every monetary system we know of (Desan, 2014). In other words, it is not only taxing states that can endow a thing with money status, but that is the historically common model. The broader point is that market relations alone cannot endow any thing with the properties that make it money; even without tax, there needs to be some collective authority in place to decide what counts as the valid discharge of an obligation, for example in the form of 'legal tender' rules (Mann, 1992).[15]

What we can draw from the Chartalist theory is this: what makes some $X$ 'money' is the set of facts which make it the case that any debt incurred in any transaction can be settled by supplying the creditor with the relevant quantum of $X$; debtors and creditors are grouped within a defined space of economic exchange wherever those facts obtain. The power to impose and enforce debt-settlements with some $X$ is, at base, the power to issue $X$ as the general equivalent. In our view, this must always presuppose and require some political, extra-catallactic forces, i.e., in the creation of the legal and institutional framework that surrounds any $X$'s function as the general equivalent.

The question then becomes: how does something become a socially accepted accounting system? While we can imagine counterfactuals in some state of nature, generally these processes occur within an organised political community—i.e. in communities managed by individuals appointed as organs of the whole. In such contexts, designation and acceptance is the prerogative of government—understood as the pooling of our common wills into, and as, an agent tasked with powers to promote and secure our common interests—although the government may act in concert with private market actors such as financial institutions (Hockett and Omarova, 2017). Granted, popular acceptance of official designation is also essential, but the real dynamic is a complex interplay of top-down and bottom-up social forces. In legal terms, it is important to note that one incident of *sovereignty* is the power to prescribe what does and does not constitute a legal settlement of a commercial debt (Mann, 1992, pp. 460–478). To that descriptive claim we can add the normative assertation that public authority must be subject to public oversight, direction and control, to ensure that it remains tethered to the common good. Only this distinguishes 'sovereignty' as a political state from 'domination' as a result of the brute power of one or few over many.

[15] Some legal tender rules, for example in French law, go so far as to criminalise the refusal to accept the sanctioned means of payment; others, for example in English law, stipulate that once a creditor refuses payment in legal tender, he cannot avail himself of the services of the state courts to enforce the debt.

In our view, privately issued 'currency competitors' such as Bitcoin cannot satisfy that requirement by themselves. The power to 'create Bitcoin' is a computational power, factual in nature because resting on the existence and control of certain technological infrastructure and its affordances. The power to issue 'currency' is a *normative* power: *a mode of authority capable of changing the facts about our obligations to one another*. Legally, this point is slippery because the principle of the freedom of contract means that I can accept 'payment' in virtually any medium you agree to (be it cans of chicken soup). Without lapsing into a legally dogmatic view, however, it is vital to remember that in the case of a failure to 'pay' in cans of chicken soup, I can seek the back-up of the organised political community through its court system and I will obtain a judgment denominated in the money recognised by that system and (only) dischargeable in that money. Designation of what is and is not 'money' is, at least in principle, a common power; it is constituted multilaterally, is fundamentally mind-dependent, and is therefore susceptible to rejection by the relevant community. Again, by saying this, we are not wedding ourselves to a dogmatically state-centric conception of money; a political community may reject the state's official currency, and may create its own unofficial one. But it is unsurprising that there is a strong empirical correlation between constituted political authority and money (Rosa, 2015). The upshot of this is that currency competition, even by private actors and networks, is always a *political* competition that necessarily implicates all other significant *loci* of social, political, and legal authority.

Because commercial exchange requires a general equivalent, everyone subject to the demands of commerce—which is to say, everyone—is dependent on, and has a stake in, the processes by which something comes to acquire the properties that make it a general equivalent. Insofar as our most basic interests are themselves at stake in commercial exchange, we all have a basic interest in the conditions under which commerce, as a system, is stabilised. The processes causally responsible for creating and circulating money are among these, perhaps chief among them. So we have *a basic shared interest* in the creation of money, which furnishes a *shared entitlement* to control over that power. If shared rights are the Hohfeldian incidents—the privileges, claims, immunities, etc—that function to promote our shared good, conceived in terms of our shared vital interests, then there is a robust normative argument that we all jointly have a right to control the processes by which money is created (Hohfeld, 1917). As Joseph Raz puts it, 'X has a right if X can have rights, and, other things being equal, an aspect of X's well-being (his interest) is a sufficient reason for holding some other person(s) to be under a duty' (Raz, 1986, p. 16).

Interestingly, the cryptocurrency project itself is premised on this kind of normative argument—how else could a private person or network of persons justify launching a disruptive new money candidate? But in virtue of its distributed, pseudonymous nature and intentional lack of responsive human governance, the Bitcoin network appears to be somewhat of a poison pill; there is no way for society to influence or control it to ensure it meets society's needs (short of rejecting it wholesale). It asserts the political prerogative to change the money system, but does so by instantiating a new money system that is immune to human intervention in perpetuity so long as the market values it.

Bitcoin is, in short, a political project, and must elicit a political response one way or the other. The interest in sovereign-issued digital currency is growing rapidly. It seems to us unlikely, however, that any central bank digital currency (CBDC) will displace Bitcoin entirely. From the first ten years, it seems equally plausible that the incumbent

monetary system will absorb Bitcoin rather than rejecting it.[16] In this context, it is convenient to note a fundamental shift in narratives surrounding the role of Bitcoin in the monetary system. In our view, these are moving from a zero-sum game (parallel existence or simple replacement through competition) to integration into the monetary system (e.g. as a reserve asset in our post-Bretton Woods system to curb the excesses of central banks' unconventional monetary policy) (Bateman and Allen, 2022).

In our view, debates that unfold over the next decade will likely determine the shape of 'money' in the century to come. From a marginal (and easily dismissible) position just five years ago, Bitcoin has become an important agent of provocation in those debates, so it is essential to understand its value proposition and proper place in the scheme of monetary theory. On the basis of our analysis, therefore, we conclude with a bill of propositions:

(i) Every 'monetary system' is predicated on a political community existing over and above the aggregate of market participants;
(ii) Political communities implicitly require some form and degree of 'organisation', being the appointment of individuals in a special capacity to act for the community as a whole;
(iii) That political community can have rights, which are borne in a representative capacity by its organs;
(iv) Each member has a vital interest, and the community has a vital interest, at stake in the structure and stability of its monetary system;
(v) Those interests constitute sufficient reason to ensure that the powers by which the monetary system is managed are under public direction; and
(vi) Whoever can help make this the case is obligated, as a matter of justice, to do so, but should not do so in a manner which precludes future generations from making further changes to the monetary system.

If these propositions are correct, it would seem that Bitcoin in particular, and 'private' monetary systems in general, are as much a normative offense as they are an ontological error.

## 5. Conclusion

We commenced this paper with the observation that technology-driven developments, including cryptocurrencies, are presently challenging existing theories of money. This provided an opportunity to apply different theories to 'new money candidates', in so doing, to stress-test those theories.

The substance of our analysis focussed on one of the central components of Bitcoin and other 'cryptocurrencies' like it: the Proof-of-Work consensus mechanism. On our analysis, those advocating Bitcoin as money (or as a *money-like* phenomenon) should base their arguments rather on a Marxian than a Mengerite theory of value. The value of a Bitcoin is more accurately described as a function of the labour time investing in 'minting' or 'mining' it through the proof-of-work consensus mechanism than in terms of a regression to prior use-value.

[16] They are generally marginal cases, and the point must not be overstated, but Bitcoin has been adopted as legal tender in certain jurisdictions including El Salvador (Jones and Aveler, 2021).

Bitcoin's bid money status, we concluded, necessarily falters on ontological grounds, and does so in a way that demonstrates the deficiencies of commodity theories of money (including Marx's). Our view could be described as Chartalist, although we would stress the legal and political foundations of money; without making any strong claims about a Weberian ideal-type state, our view does insist that the constitutional underpinnings of the sort of social phenomena that could be described as social acceptance by a market theorist of money presuppose and rely on a politico-legal substructure of some sort that is fundamentally extra-catallactic. As Bitcoin (and related proposals) seek to insulate the monetary system from political 'interference', they cannot, in our view, be argued to represent a democratisation of economic relations in any meaningful sense. The *demos* has no role in structuring that (purported) money form. In our view, the solution proposed in the Nakamoto Whitepaper reinforces private relations of economic domination more than it puts economic production and relations under a guided democratic control.

This is problematic because, on its terms, it claims to have an emancipatory agenda. It seems that the best argument one could make for Bitcoin is as *a private chartal money*, i.e. within a private payment community. But that already concedes that Bitcoin does not have a 'non-political economy'. That makes it susceptible to the critique that this 'private' money system operates within the context of a public Chartal system. To the extent that it is, or could be, parasitic on the latter, the broader community has a *prima facie* legitimate interest in regulating it. In other words, Bitcoin users cannot constitute a public community acting as one, with a locus of public authority somewhere without violating their own claim to Bitcoin's properties emerging spontaneously from market exchange among disaggregated individuals.

## Bibliography


Allen, J. G. 2019a. Negotiability in digital environments, *Butterworths Journal of International Banking and Financial Law*, vol. 7, 459–63.

Allen, J. G. 2019b. Property in digital coins, *European Property Law Journal*, vol. 8, no. 1, 64–101. doi:10.1515/eplj-2019-0005.

Allen, J. G., Rauchs, M., Blandin, A., and Bear, K. 2020. *Legal And Regulatory Considerations For Digital Assets*, Cambridge UK.

Anon. 2023. Cryptowiki. https://Cryptowiki.Net/?Title=Proof-of-Work_system (date last accessed 5th January 2021).

Assenmacher, K. and Krogstrup, S. 2018. Monetary policy with negative interest rates: decoupling cash from electronic money, vol. 191, 18. IMF Working Paper No 2018/191.

Back, A. 1997. A Partial Hash Collision Based Postage Scheme. http://www.hashcash.org/papers/announce.txt.

Bateman, W. and Allen, J. 2022. The law of central bank reserve creation, *The Modern Law Review*, vol. 85, no. 2, 401–34. doi:10.1111/1468-2230.12688.

Best, B. 2014. Bitcoin and Austrian economics. *Bitcoin Magazine*. https://bitcoinmagazine.com/culture/bitcoin-austrian-economics-1409113330 (date last accessed 27th March 2023).

Bitcoin Mining. 2023. Mining. https://www.Bitcoinmining.Com/ (date last accessed 5th January 2021).

Bitcoin Wiki. 2023. Mining. Https://En.Bitcoin.It/Wiki/Mining (date last accessed 5th January 2021).

Cambridge Centre for Alternative Finance. 2023. Cambridge Bitcoin Electricity Consumption Index. https://ccaf.io/cbeci/index (date last accessed 5th January 2021).

Cohen, G. A. 2020. *Karl Marx's Theory of History*, Princeton University Press. doi:10.2307/j.ctv105b973.

Cunningham, F. 2005. Market economies and market societies, *Journal of Social Philosophy*, vol. 36, no. 2, 129–42. doi:10.1111/j.1467-9833.2005.262_1.x.
Desan, C. 2014. *Making Money*, Oxford, Oxford University Press. doi:10.1093/acprof:oso/9780198709572.001.0001.
Douglas, A. X. 2015. *The Philosophy of Debt*, London, Routledge. doi:10.4324/9781315681009.
Dwork, C. and Naor, M. 2001. Pricing via processing or Combatting Junk Mail, pp. 139–47 in *Advances in Cryptology—CRYPTO' 92*, Berlin, Heidelberg, Springer Berlin Heidelberg. doi:10.1007/3-540-48071-4_10.
Faux, Z., and Shen, M. 2022. An $85b crypto collapse reveals a new kind of bank run, *Australian Financial Review*. https://www.bloomberg.com/news/articles/2022-05-19/luna-terra-collapse-reveal-crypto-price-volatility#xj4y7vzkg (date last accessed 27th March 2023).
Hansen, K. 2019. The Menger-Mises theory of the origin of money—conjecture or economic law?, *Quarterly Journal of Austrian Economics*, vol. 22, no. 1, 26–48. doi:10.35297/qjae.010017.
Harvey, D. 2014. *Seventeen Contradictions and the End of Capitalism*, London, Profile Books.
HM Treasury. 2022. 'Government Sets Out Plan to Make UK a Global Cryptoasset Technology Hub'. https://www.gov.uk/government/news/government-sets-out-plan-to-make-uk-a-global-cryptoasset-technology-hub (date last accessed 4th April 2022).
Hockett, R. C. and Omarova, S. T. 2017. The finance franchise, *SSRN Electronic Journal,* 1143–218. doi:10.2139/ssrn.2820176.
Hohfeld, W. N. 1917. Fundamental legal conceptions as applied in judicial reasoning, *The Yale Law Journal*, vol. 26, no. 8, 710. doi:10.2307/786270.
Ingham, G. 2004. *The Nature of Money*, London, Wiley.
Ingham, G. 2018. A critique of Lawson's "social positioning and the nature of money", *Cambridge Journal of Economics*, vol. 42, no. 3, 837–50. doi:10.1093/cje/bex070.
Innes, A. M. 2004. *Credit and State Theories of Money* in Randall Wray, L. (ed.), London, Edward Elgar.
Itoh, M. and Lapavitsas, C. 1999. *Political Economy of Money and Finance*, London, Palgrave Macmillan UK. doi:10.1057/9780230375789.
Jakobsson, M. and Juels, A. 1999. Proofs of work and bread pudding protocols, pp. 258–72 in *Secure Information Networks*, Boston, MA, Springer US. doi:10.1007/978-0-387-35568-9_18.
Jones, S. and Aveler, B. 2021. El Salvador becomes first country to adopt Bitcoin as legal tender. *The Guardian*. https://www.theguardian.com/world/2021/jun/09/el-salvador-bitcoin-legal-tender-congress (date last accessed 27th March 2023).
Keynes, J. M. 2016. *The General Theory of Employment, Interest, and Money*, New York, Houghton Mifflin Harcourt.
Kjærland, F., Khazal, A., Krogstad, E., Nordstrøm, F. and Oust, A. 2018. An analysis of Bitcoin's price dynamics, *Journal of Risk and Financial Management*, vol. 11, no. 4, 63. doi:10.3390/jrfm11040063.
Lawson, T. 2016. Social positioning and the nature of money, *Cambridge Journal of Economics*, vol. 40, no. 4, 961–96. doi:10.1093/cje/bew006.
Lawson, T. 2018. The constitution and nature of money, *Cambridge Journal of Economics*, vol. 42, no. 3, 851–73. doi:10.1093/cje/bey005.
Lawson, T. 2019. The nature of money and the possibility of cryptocurrency money, in *Cryptocurrencies and the Future of Money*. Madrid, Instituto de Empresa. https://docs.ie.edu/cgc/research/cryptocurrencies/CGC-Cryptocurrencies-and-the-Future-of-Money-Full-Report.pdf
Mann, F.A. 1992. *The Legal Aspect of Money*, Oxford, Clarendon Press.
Marx, K. 1982. *Capital, Volume 1*. Fowkes, B. (ed.), New York, Penguin Books.
Marx, K. 1993. *Grundrisse*. Fowkes, B. (ed.), London, Penguin Books.
Marx, K. and Engels, F. 2017. *The Communist Manifesto*, London, Pluto Press. doi:10.2307/j.ctt1k85dmc.
Mazzucato, M. 2019. *The Value of Everything*, London, Penguin Books.
McCauley, R. 2021. Why Bitcoin is worse than a Madoff-Style Ponzi Scheme, *Financial Times*. https://www.ft.com/content/83a14261-598d-4601-87fc-5dde528b33d0 (date last accessed 27th March 2023).
Menger, K. 1892. On the origin of money, *The Economic Journal*, vol. 2, no. 6, 239. doi:10.2307/2956146.

Menger, K. 1871. *Grundsätze Der Volkswirthschaftslehre Teil I*, Wien, Wilhelm Braumüller.
Nakamoto, S. 2008. Bitcoin: a Peer-to-Peer Electronic Cash System. Https://Bitcoin.Org/Bitcoin.Pdf. 2008.
New Liberty Standard. 2023. Exchange Rate. Http://Newlibertystandard.Wikifoundry.Com/Page/Exchange+Rate.
North, G. 2012. The regression theory as conjectural history, pp. 167–75 in Hülsmann, J. G. (ed.), *The Theory of Money and Fiduciary Media*, Auburn AL, Ludwig von Mises Institute.
Pistor, K. 2019. *The Code of Capital*, Princeton, Princeton University Press.
Proudhon, P.-J. 2011. *Property Is Theft!: A Pierre-Joseph Proudhon Anthology*. McKay, I. (ed.), Edinburgh, AK Press.
Quinn, W. and Turner, J. D. 2020. *Boom and Bust*. Cambridge, Cambridge University Press. doi:10.1017/9781108367677.
Raz, J. 1986. *The Morality of Freedom*, New York, Oxford University Press.
Roberts, W. C. 2018. *Marx's Inferno*, Princeton, Princeton University Press. doi:10.1515/9781400883707.
Rosa, L. 2015. *International Financial and Monetary Law*, Vol. 1, Oxford, Oxford University Press. doi:10.1093/law/9780199671090.001.0001.
Rothbard, M. 2009. *Man, Economy, and State*, Auburn AL, Ludwig von Mises Institute.
Rotta, T. N. and Paraná, E. 2022. Bitcoin as a digital commodity, *New Political Economy*, vol. 27, no. 6, 1046–61. doi: 10.1080/13563467.2022.2054966.
Stoll, C., Klaaßen, L. and Gallersdörfer, U. 2019. The carbon footprint of Bitcoin, *Joule*, vol. 3, no. 7, 1647–61. doi:10.1016/j.joule.2019.05.012.
Streeck, W. 2018. The fourth power?, *New Left Review*, vol. 110, 141–50.
Szabo, N. 2008. Bit Gold. Http://Unenumerated.Blogspot.Com/2005/12/Bit-Gold.Html (date last accessed 27 December 2008).
Szalay, E. 2022. EU should ban energy-intensive mode of crypto mining, regulator says, *Financial Times*. https://www.ft.com/content/8a29b412-348d-4f73-8af4-1f38e69f28cf (date last accessed 27th March 2023).
Weber, B. 2016. Bitcoin and the legitimacy crisis of money, *Cambridge Journal of Economics*, vol. 40, no. 1, 17–41. doi:10.1093/cje/beu067.
Weber, I. M. 2019. On the necessity of money in an exchange-constituted economy: the cases of smith and Marx, *Cambridge Journal of Economics*, vol. 43, no. 6, 1459–83. doi:10.1093/cje/bez038.
Yermack, D. 2013. *Is Bitcoin a Real Currency? An Economic Appraisal*, Cambridge, MA. doi:10.3386/w19747.