What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology

Lana Swartz

Published online: 22 Jan 2018.

Submit your article to this journal ↗

View related articles ↗

View Crossmark data ↗

Routledge
Taylor & Francis Group

Check for updates

What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology

Lana Swartz

Department of Media Studies, University of Virginia, Charlottesville, VA, USA

ABSTRACT
In its first decade, Bitcoin has not proven to be a practical money form for most circumstances, but it has become a staging ground for debate around the cultural role of money in society. This debate is poised between two related but ultimately incompatible techno-economic imaginaries: *infrastructural mutualism* and *digital metallism*. Each offers a theory not just of money, but also of relations, identities, and the larger imaginaries we call 'society' and 'the economy'. In particular, they offer distinct visions of what it means to be a 'peer' in a peer-to-peer money system, and perhaps, a peer-to-peer society. This article traces the pre-history of Bitcoin, as well as more recent developments, to inquire about its future, as well as the future of money more broadly.

Introduction

Since the enigmatic Satoshi Nakamoto first proposed it nearly a decade ago, Bitcoin has survived multiple bubbles of attention and value. It has undergone discursive makeovers, been visioned and revisioned, purposed and repurposed. While Bitcoin has not proven to be a practical money form in most circumstances, it has become a staging ground for debate around the cultural role of money in society.

Money, as technological arrangement, performs a relation between people in a moment of transaction as well as relations between individuals and the larger imaginaries we call 'society', 'the state', and 'the economy'. Money is a creature of network effects: it requires a community of shared belief to 'work', to exist as something recognizable as money. These beliefs are reflexively produced in the technologies of money, which are instantiations of these shared expectations. A theory of money, then, is a techno-economic imaginary, a theory of the larger social order (or a challenge to it) and a way of materially enacting that theory. What sense can we make of the techno-economic imaginaries offered by Bitcoin?

CONTACT Lana Swartz ✉ lana@llaannaa.com

In order to answer this question, I employ, as analytical methodology, an understanding of money as an instrument of shared temporality. Bill Maurer (2005, p. 89) describes how value and therefore financial instruments can only be understood in terms of 'pasts remembered, futures anticipated, and time measured'. We accept something as money because we expect that it will be accepted tomorrow. Experiments with money projects catalyze experiments with time. John Allen and Pryke (1999) draw upon Georg Simmel to demonstrate how money is a pattern and is patterned by modes of experiencing space and time. They show how derivatives and other forms of 'digital capitalism' function to 'pull distant spaces into centres of rhythmic coordination which coordinate exchange in a new form of monetised space – time' (p. 52). Finn Brunton (2017) has described how utopian currencies are 'stories of the future expressed as kinds of money' complete with 'models of history embedded in practices of value'. Money, then, is a way of performing value in the present by invoking a past and exerting it onto the future. It is always speculative, engaging in hypothesizing, and projecting a particular future. Taken as a methodology, this temporal view of money opens a more precise question about Bitcoin: What specific pasts does it pull into the present to pattern what range of possible futures?

What was Bitcoin and what will it be? This article first offers a very short pre-history of Bitcoin, tracing its origins to the cypherpunk and crypto-anarchist subcultures of the 1990s and their pursuit of a 'digital cash' technology. It describes the emergence of Bitcoin at a time of financial crisis, distrust in institutions, and surveillent business models. It looks to this context, as well as back to the cypherpunks and crypto-anarchists, to elaborate *infrastructural mutualism* and *digital metallism* as Bitcoin's animating techno-economic imaginaries. The next section looks at key developments in Bitcoin – namely, tensions between hobbyist and industrial miners and between price and payment – to demonstrate the ultimate incompatibility of these techno-economic imaginaries. An important theme throughout is the question of what it means to be a 'peer' in a 'peer-to-peer' money technology. Finally, this piece speculates about tensions between these techno-economic imaginaries, the future of Bitcoin, and perhaps the future of money, technology, and the relations they perform.

What was Bitcoin?

A short pre-history of Bitcoin

Bitcoin did not emerge spontaneously in 2008. Instead, its origins can be traced at the very least back to the 1990s, when those interested in the potential of cryptography and related technologies for social and political change converged as a community on online and offline fora, notably over email

on the Cypherpunks mailing list, which was formed in 1992.[1] The group was spurred by developments decades earlier that democratized access to state-of-the-art cryptography. These include the 1967 publication of David Kahn's *The Codebreakers*, which controversially included details of National Security Agency practices that had otherwise been kept secret; the 1975 release of the U.S. Department of Commerce Data Encryption Standard, a cypher that could be used to transmit non-classified data; and the release of public-key cryptography in 1976 followed by the RSA asymmetric cypher in 1977 (Levy 2001, Blanchette 2012). These developments meant that strong cryptography was now possible with relatively modest computing systems. Cryptography, previously a weapon of the state, had begun to seem like a means of technological empowerment for the individual.

The list members were invested in freedom and autonomy, broadly defined. They believed that technology could be the key to a future free society, and they saw 'digital cash' as an essential component of this vision. They were not, however, homogenous in their political ideologies. The 'Cyphernomincon', a Frequently Asked Questions of sorts about the email list by co-founder Tim May (1994), described its members as a mix of 'radical libertarians, some anarcho-capitalists, and even a few socialists'. As May put it in a post to the mailing list in 1993, 'Though not all on the Cypherpunks list are anarchocapitalist libertarians. Many are just interested in privacy, others want to see power taken away from multinational corporations, and so on.'[2]

While it is difficult to draw clear boundaries around the subjectivities present, it is analytically useful to tease out unarticulated distinctions between two that emerged from this milieu: *cypherpunk* and *crypto-anarchy*. Computer scientist Arvind Narayanan (2013, p. 76) makes a similar distinction. He describes it succinctly:

> For cypherpunks, crypto was at the core of a vision of how technology would cause sweeping social and political change, weakening the power of governments and established institutions. A closely related term is crypto-anarchism, a political philosophy that, in its idealized form, recognizes no laws except those that can be described by math and enforced by code.

In the following sections, I will briefly elaborate this distinction in order to set up its application to Bitcoin. I will also consider the efforts of both cypherpunks and crypto-anarchists to develop 'digital cash' systems prior to the advent of Bitcoin.

Cypherpunk

The term 'cypherpunk', coined by Jude Mihon in the early 1990s, is a portmanteau of cipher and punk (*Modem Grrrl* 1995). It referred to a range of activists who believed that privacy is, above all other things, the foundation of a free society. The 1993 'A Cypherpunk's Manifesto', written by Eric Hughes, one of

the founders of the Cypherpunks email list, defined privacy as 'the power to selectively reveal oneself to the world'. Privacy, in this sense, was defensive and informational: individuals should be able to freely conceal and express information about themselves. To the cypherpunks, privacy was a natural right: authorities could not bestow it, but they could take it away. Privacy, then, was also fragile. It could easily be lost if informational infrastructures were controlled by entities that did not value it. The only way, from this point of view, to protect privacy was to produce cryptographic information systems outside of the purview of government or corporate entities. The design of information protocols is the design of the larger social contract.

The cypherpunks saw themselves as a vanguard. Because they were equipped with the technological skills and the political commitments necessary to do so, cypherpunks felt it was up to them to protect privacy. In his manifesto, Hughes (1993) wrote, 'Cypherpunks write code', meaning, essentially, that they would produce the technologies that would enable and constrain the basis of communicative reality. 'Cypherpunks write code' means that cypherpunks are obliged to help produce systems that would, as proto-cypherpunk computer scientist David Chaum had put in 1985, 'make big brother obsolete'.

To 'write code' was to produce not just technology but to produce the protocols through which privacy, and therefore communicative reality, would be executed.

Although the cypherpunks were in the privileged situation of being equipped to 'write code', their aims were simultaneously individualistic and populist. They recognized that communication privacy did not function at the level of the individual: no one could have it unless everyone did. Hughes (1993) wrote, 'We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it.' Hughes' (1993) manifesto emphasized that 'people must come and together deploy these systems for the common good', to develop and use shared communication systems that would form the basis of a new society predicated on privacy.

Crypto-anarchy

Crypto-anarchy extended cypherpunk's logic of free expression to free markets. The political project of crypto-anarchy extended beyond the pursuit of privacy. The crypto-anarchists believed, as Tim May wrote in his 1994 'Cyphernomicon,' that cryptography offered, 'the building material for a new age' but one based on an 'anarcho-capitalist market system'. In a 1992 version of 'The Crypto Anarchist Manifesto,' an ironic mimic of 'The Communist Manifesto,' May addressed 'Cypherpunks of the World', hoping to bring them over to the crypto-anarchist vision.

Crypto-anarchists believed that freedom – free as in speech and free as in markets – would be accomplished through cryptographic technology that enabled voluntarist, mutually beneficial contractual relationships. These relationships would form markets that would, in aggregate, become the key organizing system for society. Collective needs would be met through this network of markets, a vision that May described as a 'throwback to the pre-state days of individual choice about which laws to follow' (1994). Unlike the current capitalist system, crypto-anarchists believed, as Duncan Frissell put it in a post to the Cypherpunk email list in 1996, that 'future market societies [would] no longer be in the hands of "The Authorities" but is rather in the hands of those trading on the market; i.e. everyone on earth'. To Frissell and other crypto-anarchists, mass participation in such markets would mean the 'deregulation of human behaviour'.

Crypto-anarchy was less inclusive than cypherpunk. It mattered little that not everyone would be able to equally participate in the coming, as May (1993) put it, 'Galt's Gulch in cyberspace', a reference to Ayn Rand's fictional libertarian heterotopia. Frustrated with anti-discrimination laws and other inclusive features of liberal democracy, he argued that 'choice was no longer allowed' and equated democracy with 'mob rule' (May 1994). Whereas cypherpunks often framed their work as deploying code for the preservation of the natural right to privacy for all, the crypto-anarchist position celebrated inequality through meritocracy. The 'masses', May (1994) wrote, would not need to be converted. Rather, crypto-anarchy would be something that would 'just happen' to them, just as 'world financial markets, derivative instruments' had before. Each individual would be responsible for seizing the intellectual and technological tools necessary to succeed in the coming society.

Digital cash

Money as a technology was an important building block of both the cypherpunk and crypto-anarchist visions. For cypherpunks, being able to selectively reveal personal financial and transactional information was one of the most powerful forms of privacy. For crypto-anarchists, having a money system untethered to governments was necessary for a truly free market society. Over the last decades of the twentieth century and the first decades of the twenty-first, there were several attempts to design and implement systems that would accomplish some these goals: 'digital cash'. Some proposals emphasized the cypherpunk position, namely the desire to build shared decentralized infrastructures for transactional privacy. Others adhered more closely to the crypto-anarchist view that a money authorized by something other than governments was the key to a new, liberated market society.

Polymathic computer scientist David Chaum's work, particularly his 1985 paper describing an electronic cash system that promised to 'make big brother obsolete', which later formed the basis for the company DigiCash,

was an important touchstone. In 1996, May described a fictional cryptographic black market called 'BlackNet' powered by 'CryptoCredits'. In 1998, computer scientist Wei Dai published a description of an anonymous, distributed electronic cash system, which he called 'bmoney'. In the late 1990s and early 2000s, Nick Szabo developed a proposal for 'bit gold', a system in which computers 'mined' for 'scarce' digital commodities (Szabo 2011). These systems drew from the visions of cypherpunks and crypto-anarchists alike, but none was able to achieve them.

The emergence of Bitcoin

By early 2000s, the excitement around both cypherpunk and crypto-anarchy had cooled. John Gilmore, one of the list's founders, declared it dead in 2001 (Rodger 2001). While advances were made in academic and commercial cryptography, little new work was being done in 'crypto for privacy' (Narayanan 2013, p. 75). Then, in 2008, an individual or group using the pseudonym Satoshi Nakamoto posted to a different, largely non-political cryptography email list a white paper outlining a new system for digital cash called Bitcoin. Bitcoin, along with projects like TOR and WikiLeaks, was welcomed as a renaissance.

Shortly after the publication of the whitepaper, Satoshi and members of the email list began a Free and Open Source software project to implement the proposed system. In 2009, the first Bitcoin client was released, and Satoshi mined the first 'genesis block' of 50 Bitcoins. In the spirit of the 1990s Cypherpunks email list, the conversation about the technical and philosophical dimensions of Bitcoin was spirited. On Bitcoin email lists and forums, veterans and newcomers revived the conversation around cypherpunk and crypto-anarchy.

Since the Bitcoin whitepaper was first released in 2008, there have been flurries of intense interest in unmasking the mysterious Satoshi Nakamoto, as if his – hers? their? – identity were the key to understanding the origin of Bitcoin. Indeed, Bitcoin, like all socio-technical systems, was a collective effort. It was out of a decades-long asynchronous conversation at the intersection of cypherpunk and crypto-anarchy, which took the form of both writing words and writing code, that the technical elements and the ideological positions that would become Bitcoin emerged. As someone using an email address linked to Satoshi[3] wrote on a Bitcoin development email list in 2015, after another supposed Satoshi had been unveiled, 'We are all Satoshi'.

What is Bitcoin?
At nine pages, Satoshi's paper detailed a system that uses a decentralized, peer-to-peer network to produce and transmit value tokens. The proposed system outlined three of the key features necessary for maintaining a cryptographic currency on a distributed digital network. Bitcoin included a currency

token (a Bitcoin), the payment rails for exchanging those tokens (Bitcoin), and a distributed ledger-keeping protocol (the blockchain).

Simply put, as Satoshi did in his 2008 whitepaper, Bitcoin is 'a purely peer to peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution' (p. 1). As with cash, in the Bitcoin system, the payer sends a value directly to the payee. This is accomplished using public-key cryptography. The sender hashes a transaction with their private key and the recipient's public key, assigning ownership of Bitcoins to the recipient. This transferral is broadcast, without any identifying information, on the blockchain, the system's decentralized public accounting ledger. The blockchain also prevents the so-called double spending problem, copying a Bitcoin and using it more than once. This eliminates the need for a third party, like a bank, to oversee and verify the transactions.

As with cash, the identities of the payer and payee could remain unknown to each other and to the public. In the whitepaper, Satoshi Nakamoto (2008) called this a 'new privacy model' (p. 6). In traditional payment systems, financial institutions keep track of identities and transactions, all of which are hidden from public view. In Satoshi's new model of privacy, the blockchain is a public record of all transactions, but the identities associated with those transactions are hidden from public view.

In this originary version, by running the blockchain and participating in the Bitcoin network, users 'mine' Bitcoins for their own use. Users can gain Bitcoins in three ways: by 'mining' them, by accepting them in exchange for a good or service, or by trading currency for them. Bitcoin was designed with a hard upper limit on the total number of Bitcoins that can ever be mined, about 21 million. This limit serves as monetary policy enacted in code, with the goal of hard-coding a currency that is, as Bitcoin advocates put it, 'inherently deflationary' (see, for example, Antonopolous 2015, p. 178). The amount of Bitcoins that are awarded for mining decreases at a set rate, mimicking the increasing scarcity of commodity mining.

Bitcoin's techno-economic imaginaries

Bitcoin debuted at a historical conjuncture ripe for change in the practice of money. The year 2008 is marked as the unfolding of the global financial crisis, which undermined the popular trust in and the legitimacy of government institutions and the mainstream financial system. This time was defined by the ubiquity of social media business models that codified and enclosed relations as 'social data' to be mined for value.

These two factors - information surveillance and financial instability – opened up money for rethinking in terms of two imbricated but, I will argue, ultimately quite distinct techno-economic imaginaries: infrastructural

mutualism and digital metallism. These positions resonate in perfect pitch with cypherpunk and crypto-anarchy, and they amplify the distinctions between these two originary visions. Infrastructural mutualism and digital metallism, like cypherpunk and crypto-anarchy before them, are not discrete, opposing ideologies. Rather, they represent two analytically distinct techno-economic imaginaries. Sarah Jeong (2013, p. 27) describes Bitcoin as a 'distributed constitutional project'. From these two points of view, what kinds of social order might it constitute?

Previously, with my co-authors, I have characterized Bitcoin in terms of digital metallism (Maurer *et al.* 2013). The concept of Digital Metallism has been noted and elaborated by scholars (e.g. Bjerg 2015, Ferry 2016, Mezzandra and Neilson 2017, Zimmer 2017) and even within the Bitcoin community itself.[4] But while digital metallism characterizes one of the dominant techno-economic imaginaries of Bitcoin, it does not account for the full range of interest in it. Nigel Dodd (2017, p. 3) makes a similar point when he argues, 'There is not one Bitcoin, but several'. In the following section, I provide a gloss on our previous articulation of digital metallism, and trace its connections to crypto-anarchy. Then, I articulate *infrastructural mutualism* as a covalent techno-social imaginary aligned with cypherpunk.

Digital metallism

Bitcoin's 'digital metallism' is 'metallist' in that embraces a theory of money in which the only truly sound money is one backed by a commodity like gold, which derives its intrinsic value from the market. Otherwise, its value is open to manipulation by financial and state actors. Crucially, Bitcoins are 'mined', not 'minted'. They are not, like state currencies, uttered from a central authority. Rather, they are won by crunching numbers. As Zac Zimmer (2017) points out, there is no technical reason why the system should work this way; instead, it is an ideological choice that Satoshi built into the Bitcoin architecture.

A range of classical figures as diverse as Adam Smith, Karl Marx, and Carl Menger have theorized that money's origins lay in its commodity form. More recently, a consensus has developed across fields among scholars such as Christine Desan (2014), Nigel Dodd (1994, 2014), David Graeber (2001, 2011), Keith Hart (1986, 2001), Michael Hudson (2004), and Geoffrey Ingham (1996, 2004), that money more likely developed (and, indeed, continues to function) as a way of keeping track of obligations between individuals and governing institutions and, ultimately, as a vector of state power. Nevertheless, the commodity theory of money remains influential among both mainstream neo-classical economists and Bitcoin's digital metallists.

Bitcoin, from a digital metallist point of view, proposes to be a new, fundamentally crypto-anarchist kind of money, 'apolitical' and untethered from fallible institutions, and firmly rooted, instead, in an idealized vision of 'the

market'. The digital metallism of Bitcoin is informed by classic economic liberalism, which advocates that a money supply be determined by international currency markets rather than state policy, as well certain veins of libertarianism, which advocate extra-national money, free from state taxation or control (Karlstrøm 2014, Golumbia 2016).

Digital metallism is evident in the earliest descriptions of Bitcoin. In a 2009 message board comment announcing the Bitcoin project, Satoshi wrote, '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.' A diverse range of Bitcoin advocates expressed similar sentiments. WikiLeaks founder and member of the original Cypherpunks email list Julian Assange said of Bitcoin, 'One does not need to trust any central mint.'[5] Eclipsed Facebook co-founder turned Bitcoin investor Tyler Winklevoss said, 'We have elected to put our money and faith in a mathematical framework that is free of politics and human error' (Popper and Lattman 2013).

Digital metallism, as a techno-economic imaginary, is a theory not just of money but of society. It confers identities and modes of interaction. For digital metallists, this gives Bitcoin an autonomy of value external to a centralized authorization authority. The autonomy of Bitcoin's value is transmuted into autonomy for those who use it to trade as peers. Metallists, both digital and geologic, crave a money and therefore a sense of personal agency characterized by what Ferry (2016, p. 58) calls 'immediacy': that 'does not mediate, nor does (or perhaps, nor should) anything mediate on its behalf'. Rafferty and Bryan (2006) demonstrate how, in the mainstream financial industry, derivatives function, as gold once did, to anchor and commensurate varied forms. Bitcoin's digital metallists see Bitcoin as serving the same function, but with even greater 'immediacy'. From this point of view, Bitcoin is a self-sovereign currency, and those who truck in it are, as is desirable from a crypto-anarchist point of view, self-sovereign individuals.

Digital metallism puts an emphasis on the priced value of Bitcoins. That value is seen as the natural outcome of a market. In this view, Bitcoin is a store of value that is deflationary, cannot be manipulated, and is easy to hide from taxation. This emphasis on value, expressed as price, also makes it seem like an interesting speculative opportunity. Wealth in Bitcoins is seen as an investment in a future when the world's governments have either become too unstable to manage the money supply, too powerful to respect private property, or both.

From this perspective, Bitcoin is best used not as 'digital cash' used to transmit value free from surveillance, but as 'digital gold' used to invest in a coming crypto-anarchist future. For digital metallists, Bitcoin functions like a prediction market: investing in it is a bet against institutions and in favour of crypto-anarchy. It draws from the past to conjure the crypto-anarchist vision as a looming near future. It allows you to stake your claim: What do

you think is coming and who do you want to be when it comes? In the meantime, of course, you might just make a quick buck buying and selling those stakes to others. As I will demonstrate in the following sections of this paper, digital metallism set the stage for Bitcoin to become, like gold, a speculative instrument rather than an everyday payment system.

While Bitcoins operate like nuggets of digital gold, they are only able to do so because they are 'records' in the blockchain. The term digital metallism, then, encompasses the unexpected dualities that animate the value of Bitcoins: both materiality and virtuality, both commodity and credit theories of money. As my collaborators and I (Maurer *et al.* 2013, p. 263) write:

> trust in the code substitutes for the (socially and politically constituted) credibility of persons, institutions, and governments. It is this – not the anonymity or the cryptography or the economics – that makes Bitcoin novel in the long conversation about the nature of money.

For digital metallists, the value of a Bitcoin is rooted in 'trust in numbers', both in the market and in the math – and, implicitly, the community that makes both possible. Indeed, it is precisely this polysemy that allows other techno-economic imaginaries to function alongside digital metallism. Namely, what I call *infrastructural mutualism*.

Infrastructural mutualism

Digital metallism does not sufficiently account for the full spectrum of interest in Bitcoin. I would like to augment it with a rendering of another key techno-economic imaginary: *infrastructural mutualism*. From this perspective, which finds its origins in the cypherpunk ideology of privacy and mutualistic self-help organized through 'writing code', Bitcoin is not primarily an alternative to state-backed money but an alternative to private payment intermediaries that seek to control and survey its passage. It affords a cooperativist vision of a money technology and therefore society.

In addition to concerns over economic crisis, much of the early interest in Bitcoin was related to its new model of privacy. To cypherpunks, in contrast to crypto-anarchists, liberty is not attained through freedom of markets but through freedom of information. Information, to use a phrase familiar to cypherpunks, 'wants to be free'. Free, that is, to move unhindered by third-party interference, control, or surveillance. To infrastructural mutualists, Bitcoin is a decentralized platform to move money, which is just another form of information. This is distinct from the instrumentalist desire for clandestine traffic in illegal or unsavoury goods. It is privacy for the sake of individual and collective autonomy.

The infrastructural mutualist position represented in a 2011 blog post by Rainey Reitman of the EFF, a digital civil liberties organization co-founded by cypherpunk John Gilmore, which described Bitcoin as a 'step toward

censorship-resistant digital currency'. Reitman emphasized that Bitcoin was a 'peer-to-peer digital currency system that endeavours to re-establish both privacy and autonomy by avoiding the banking and government middlemen'. Reitman was cautious about the 'ever-fluctuating market value of Bitcoin'. She did not describe this as a speculative opportunity and instead grouped speculation, along with concerns about security and mass adoption, as part of the 'uphill battle' that Bitcoin would likely face.

From the cypherpunk perspective, it's possible to advance a theory of money as fundamentally infrastructural. The politics of money are rooted in its communication, in the material control of the rails through which transactions are conducted. Transactions are literally *trans*-actions, movements across. The technology through which this movement occurs is an important vector of relations that may produce either freedom or tyranny. The value of decentralization, then, is that there is no single, unified site of control that can wield communicative power over the metaphorical 'pipes' and what flows through them. As a mutualist infrastructure, the politics of Bitcoin are analogous to the fight for network neutrality, the principle that Internet service providers should not favour or block certain content, users, or websites. The communication politics of infrastructural mutualism relate both to what James Carey (1989, p. 23) calls the transmission and ritual views of communication: the means through which value moves from one information 'place' to another is also the 'symbolic process through symbolic process whereby reality is produced, maintained, repaired, and transformed'.

For infrastructural mutualists, the surest way to produce an infrastructure for free communication – payment or otherwise – is to decentralize it, to put infrastructure in the hands of its users. Bitcoin is appealing, then, because there is no consolidated intermediary conducting transactions. Instead, all participants run a node in the network. Or, at least, as Hal Finney, the well-known computer scientist who worked on the early Bitcoin code, received the first Bitcoin transmission from Satoshi, and who had, decades before, been a regular poster on the Cypherpunks email list, put it to the Bitcoin email list in 2008, 'the long tail of node operators is sufficiently large that no small collection of nodes can control more than a small fraction of overall resources'. In this scenario, he wrote, 'the Bitcoin system turns out to be socially useful and valuable, so that node operators feel that they are making a beneficial contribution to the world by their efforts'. Node operators would be incentivized not just by the potential to 'mine coin' but by the fact that doing so enables Bitcoin to exist. The primary role of Bitcoin 'miners' is not as speculators panning for digital gold but as keepers of a decentralized infrastructure maintained for the collective good.

Whereas digital metallists were focused on price, infrastructural mutualists were focused on flow. Whereas digital metallists were invested in market-based systems that would ensure self-sovereignty, infrastructural mutualists

were invested in cooperative infrastructures that would ensure privacy. Being a 'peer' in a 'peer-to-peer' system, in the ideal infrastructural mutualist scenario, means being an active participant as a node in the Bitcoin system. This technical role is a metonym for a broader social role, one that conjures a society in which the work of what Andrew Russel and Lee Vinsel (2016) theorize as 'maintenance': the essential but boring work done by custodians of information systems. In the mutualist view, everyone does their part, rather than outsourcing this work to the tech industry for the rather dear price of informational privacy and therefore liberty. After all, for cypherpunks, no one can have privacy unless everyone does. And, indeed, cypherpunks 'write code'—usually as part of Free and Open Source Software projects— collaboratively.

Tensions in Bitcoin's techno-economic imaginaries

While digital metallism and infrastructural mutualism were deeply imbricated at the emergence of Bitcoin, these two techno-economic imaginaries acted upon Bitcoin – its community, its uses, and its technology – in ways that lead to tensions that, at present, seem insurmountable. In the following sections, I will trace how these tensions centre around two conflicts: *between individual and industrial miners* and *between price and payment*.

Between hobbyist and industrial miners

As previously indicated, in the most technical sense, a 'peer' in the Bitcoin network is a computer that is running a 'full node'. By running a full node, 'miners' both support a complete copy of the distributed blockchain, which keeps a record of the ownership and transmission of Bitcoins, and, at least until they are depleted, have the opportunity to be rewarded in Bitcoins. This process, at the centre of Bitcoin's ingenuity, would turn out to be a key site of tension. Digital metallists understood the act of mining as an opportunity to extract the greatest amount of Bitcoins to be used as a store of speculative value, whereas infrastructural mutualists saw mining as an act of collaboration to produce a shared privacy-protecting payment network.

   As interest in the value of Bitcoins grew, there was greater interest in mining itself as an act of speculation. Those prospecting for digital gold engaged in a technological arms race in mining equipment and, ultimately, undermined the capacity of individuals to run the blockchain as a distributed, mutualist infrastructure. But, for a brief period of time, many believed that Bitcoin could be run using personal computers. Finney, in his 2008 mailing list response to Satoshi's whitepaper, imagined that miners would operate 'similar to the various "@Home" compute projects where people volunteer

their compute resources for good causes'. This is an infrastructural mutualist vision of Bitcoin: voluntary contributions support a platform for the shared benefits of the co-operators. But it did not last long.

At the beginning, it seemed that Bitcoin's infrastructural mutualism and digital metallism could be compatible, even complementary – just as cypherpunks and crypto-anarchists had been. The mutualist infrastructure would provide rails for the circulation of a metallist digital commodity token. These two activities could coexist together in Bitcoin, running on a distributed network of node computers. But very quickly, interest in mining Bitcoins for their speculative value overwhelmed support for Bitcoin as a mutualist infrastructure. In the following sections, I will lay out technological shifts that illustrate the growing tensions.

From CPUs to ASICS

Within a year of the release of the Bitcoin protocol, few people running it considered Finney's vision – that Bitcoin could be contained to spare computing cycles on a multi-purpose computer – viable. By 2010, some miners discovered that Graphics Processing Unit chips, components that were developed to power high-quality graphics for computer games, could much more efficiently mine Bitcoins than a computer's Central Processing Unit (Popper 2015, Vigna and Casey 2016). Soon, the Bitcoin community developed an open-source software optimized for GPU processing that was free for anyone to use. This marked the era of 'mining rigs', elaborate homebrew assemblages of computers, crunching away in the basements and dorm rooms of Bitcoin enthusiasts. According to Bitcoin lore, these were even used to heat homes during winter, partly to defray the cost of electricity used in the process of mining.

By 2012, as Bitcoin began attracting attention, more people became interested in mining the currency. As hype spread, companies began designing more advanced hardware, including Application Specific Integrated Circuits, or ASICs, purpose-built to mine Bitcoins. Unlike the DIY GPU rigs, the ASICs were 'plug and play' devices. As described in *Wired*, 'You plug one of these machines into your computer, run special mining software, and sit back and wait for the Bitcoins' (McMillan 2013).

These ASICs worked well, perhaps too well. They turned over blocks faster, ramping up the difficulty of mining for others. As more computational power was put into confirming blocks, the difficulty increased, making former technology obsolete. Because the technology was advancing so quickly, miners had to update their equipment regularly or get left behind. In many cases, individuals sunk tens of thousands of dollars into mining equipment that would never bear a return (Schneider 2015).

From pools to factories

As the community grew, some Bitcoin miners began to devise ways to join forces and share the rewards of mining. In 2010, Slush's Pool became what is likely the first 'mining pool'. A post that year to the Bitcoin forum titled, 'World's First Mining Pool', introduced the idea by explaining the benefits of pooled mining:

> If you set out mining on your own, it may be a long time before you can make a return. Pooled mining allows you to receive smaller, more frequent, steadier payouts instead. If you have a slower computer, or a CPU miner, then pooled mining may be the only way that you will ever mint any Bitcoins at all.

Pools were a way for miners without specialized equipment to participate in mining, despite its increasing difficulty. It was decentralized cooperation, initially, a mixed digital metallist and infrastructural mutualist effort: a collaborative way to prospect for Bitcoin as a commodity and power the blockchain in the process.

But while pools initially democratized mining, they also undermined some of larger infrastructural mutualist goals of Bitcoin. Prior to the emergence of pooled mining, each computer 'running Bitcoin' was 'full node', both mining for Bitcoins and validating a copy of the Bitcoin blockchain. With pooled mining, each computer in the pool instead became part of one super-node. While the centralized computers running the pool validated the blockchain, all the member computers just mined for Bitcoins. This meant that while there were individual users engaged in mining at greater power, leading to increased difficulty and decreasing the likelihood of 'finding' a Bitcoin, there were proportionately fewer full nodes. But without enough full nodes, it is impossible to validate and relay transactions (Cawrey 2014). According to the description on the now-defunct website of the Nodeshares initiative, a Bitcoin non-profit launched in 2014 to try to increase the number of full nodes, 'without full nodes, there is no Bitcoin'.

Not all pools were created to level the mining playing field. ASIC manufacturers not only sold equipment to consumers but also used the stock equipment to build powerful centralized mining pools (Bradbury 2014). Well-capitalized groups began to set up networks of warehouses that effectively functioned as centralized mining pools in locations such as Northern China where energy costs were low (Popper 2013). One documentary profiled a Bitcoin mining complex in China owned by four people that purportedly generated 4050 Bitcoins, or $1.5 million, a month (Franco 2015). According to the documentary, the factory marshalled eight petahashes per second of computing power, accounting for 3 percent of the entire Bitcoin network. Mining continued to consolidate and by 2013, according to the information on pools compiled by the website blockchain.info, the top two mining pools operated over 50 percent the blockchain and the top five mining pools operating up to 80 percent.[6] Individual miners just could not compete.

Today, there is on-going, as yet unresolved strife in the Bitcoin community about how it will scale to accommodate large numbers of transactions. The term "miners" now refers to a profession, an industrial class of datacentre operators, most of whom are located in China (Peck 2017). Stakeholders in Bitcoin are described either as 'miners', who run the large-scale mining system, 'developers', who maintain the software, and 'investors' who own and trade in Bitcoins. De Filippi and Loveluck (2016, p. 1) have characterized this conflict as a full 'crisis of governance' between 'governance by the infrastructure', which empowers the industrial miners and 'governance of the infrastructure', which empowers the developers. The conflict is complicated, with many solutions being posed and many factions, but no one in the Bitcoin community today imagines the possibility of mutualist participation: that individuals who own Bitcoin might be peers in the act of maintaining the blockchain.

Between price and payment

The first 'real-world' Bitcoin payment, an infamous 10,000 Bitcoin order for Papa John's pizza in May 2010, was actually predated by the first Bitcoin exchange rate, which was calculated using the cost of energy spent on mining by New Liberty Reserve in October 2009. It is also predated by the first Bitcoin currency exchange, The Bitcoin Market, established in March 2010. These details from the early history of Bitcoin demonstrate one of the key tensions among Bitcoin enthusiasts: between infrastructural mutualists who believe that its most powerful function is as an everyday medium of private exchange and digital metallists who see it as a speculative instrument. The exchange function of Bitcoin – whether as a payment or a commodity – is one of the main sites where the communicative politics of Bitcoin are played out. The following sections demonstrate moments of tension in the pragmatic politics of Bitcoin's flow, decisive moments wherein users decided how it would circulate and for what kind of purposes. The chronology of early Bitcoin practices – the development of an exchange rate and currency market before any 'real-world' transaction – foreshadowed how tensions between price and payment would evolve. In most cases, speculation in Bitcoin as a commodity has overwhelmed and undermined its potential for use as an infrastructure of exchange.

Payment, political and mundane

Many early Bitcoin enthusiasts valued not just free-flow but ordinariness in payments. Infrastructural mutualists wanted to standardize mundane transactions, make Bitcoin work for the everyday before it faced major tests. But when, in 2010, the information activist organization WikiLeaks was embargoed by all mainstream payment intermediaries, some in the then-nascent

Bitcoin community called for aid to WikiLeaks and to accept payments on its behalf (Benkler 2011). Many were wary of involving Bitcoin in such a high-profile, potentially high-risk cause. One poster on the Bitcointalk forum posted in response to a 2010 thread titled, 'Wikileaks contact info?', 'I say, we MUST get it accepted at the local grocery store. … BEFORE it gets accepted at WikiLeaks. Then, we'll have a chance.' Satoshi, in particular, was not happy with the association with WikiLeaks. He posted to the same thread:

> No, don't 'bring it on.' The project needs to grow gradually so the software can be strengthened along the way. I make this appeal to WikiLeaks not to try to use Bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage.

This appears to be one of Satoshi's last posts on the forum, after which he seemingly disappeared entirely, leaving his store of Bitcoins untouched. Although it is unclear how many donations actually flowed to WikiLeaks through Bitcoin, the story was picked up in the popular press. Those who were concerned that Bitcoin could receive much – perhaps too much – attention if associated with WikiLeaks were correct. Beginning in early 2011, there was a tremendous surge of interest in and mainstream coverage of Bitcoin.

Spending and speculating

In the wake of this coverage, Bitcoin received a wave of new enthusiasts. News media covering the story highlighted the use of Bitcoin as anti-state money, a way to evade taxes, and maybe become a 'Bitcoin billionaire'. Bitcoin exchanges proliferated and thousands of new users entered the economy and began to participate in the online forums. While some experienced digital metallist or crypto-anarchist awakenings, many new entrants into the Bitcoin market treated Bitcoin as a 'get rich quick' scheme. Speculative trading was rampant.

Discussion on the fora and email lists shifted from primarily being about the development, implementation, and maintenance of the system, to being about the price of Bitcoin, who was bullish, who was bearish, and why. Trading drove up the price, which, in turn, attracted popular attention to Bitcoin. The higher the price of Bitcoin rose against the U.S. dollar, the more it seemed to prove that Bitcoin was a success. High prices seemed to legitimize Bitcoin, drive trading, and subsequently fuel future price increases. The boom of attention and speculation was self-reinforcing.

Many in the Bitcoin community were no doubt happy to see their investment rise, but not everyone was comfortable with this new-found 'success'. As one poster on the Bitcoin forum lamented on a thread titled, 'Thought experiment: Is Bitcoin a Ponzi Scheme' in 2011: 'It seems to me that people using Bitcoin is more important than people investing in Bitcoins.' Some

posters on Bitcoin forums criticized 'hoarding', and were concerned that the volatile price might discourage the use of Bitcoin for everyday payments. In response to the 'Ponzi Scheme' post, one poster described using Bitcoin from the perspective of parties to ordinary commerce:

> From customers perspective: Why should I spend my Bitcoins to buy an iPad today if the price of Bitcoin goes up every day? I keep my Bitcoins they might go up 1000%.

> From webshops perspective: Why should I accept Bitcoin as a currency if the price is volatile? I might sell my products with a loss if the BTC price drops after I sell my product and want to convert the revenue to USD.

Others were more hopeful, arguing that the speculation was just a growing pain of the young currency. One poster on the 2011 'Ponzi Scheme' thread suggested that as awareness and adoption of Bitcoin grew, it would become more self-contained, more immune to markets for trade to government currencies, at which point its infrastructural mutualist value as a payment system would become apparent, 'As a currency, it doesn't matter what the absolute price is vis-a-vis the dollar or whatever. People will be attracted to Bitcoin for a variety of reasons, including its low transaction cost and decentralized and pseudonymous nature.'

One infrastructural mutualist, in his 'Bitcoin Manifesto' posted in 2011 to Bitcoin Forum, hoped that the greed displayed by some of his fellow early adopters would simply be the 'the shit that fertilizes some beautiful flowers'. He argued that Bitcoin provided an alternative to mainstream 'flow capitalists' who did little but control infrastructure and charge rents on it, constituting a 'middle-man mafia' that was 'strangling the world'. When another poster suggested that Goldman Sachs was foolish not to 'invest' in Bitcoin, he was quick to respond:

> 'Invest' is the kind of word that the flow capitalism uses. We, as hackers, know, that it's possible to create complex software even without any outside investment at all. Now, what Bitcoin needs to show the world, is that there are alternatives in hoarding capital and creating megaprojects with huge investments.

From this point of view, Bitcoin was an opportunity to produce a new kind of infrastructure, one that should not require 'investment' in the Goldman Sachs sense. The point was not to buy in early at a low price and watch that investment pay off in form of financial dividends. Instead, 'investing' in the infrastructure of Bitcoin meant becoming part of a community and benefiting from the mutual aid it offered.

Professionalized Bitcoin trading

As the price of Bitcoin rose, there was rapid professionalization in the Bitcoin ecosystem, such as the founding of Bitcoin start-ups, Bitcoin start-up

incubators, professional Bitcoin conferences, and Bitcoin news outlets. Most of these were focused on the market dynamics of Bitcoin, on facilitating their purchase as speculative investment.

In November of 2013, according to listings on Coinbase and BitStamp (USD), 2017, the price soared to a then-high of U.S. $1162, up from just U.S. $13.36 in January. Those who owned Bitcoin spoke regularly of how 'stupid' you'd have to be to spend them, how sad it was that someone had once spent 10,000 Bitcoins on Papa John's pizza. That same year, the Bloomberg terminal began to offer a Bitcoin price ticker (Dillet 2013). It seemed that speculation in Bitcoin as a commodity had fully overwhelmed its capacity to serve as an infrastructure for everyday payment.

A few Bitcoin payment intermediaries arose, offering to make payments in Bitcoins easier for merchants to accept. These usually acted as a brokerage, taking Bitcoin from consumers, giving state currency to vendors, then speculating on the price of Bitcoin themselves. High-profile tales of big companies accepting Bitcoin were actually just using these intermediaries and endorsing Bitcoin at little risk or expense (Davidson 2015). Instead of the disintermediation of money, Bitcoin was practised as a new hyper-marketized form of mediation. Every payment was an act of arbitrage for someone. As in Hardin and Rottinghaus's (2015) description of mainstream finance, mediation and arbitrage were inextricable in Bitcoin.

In 2014, in line with existing practice, the Internal Revenue Service issued guidelines that, for tax purposes, treated Bitcoin as property, not as currency or an exchange platform. This meant that Bitcoin would be subject to capital gains taxes, making it difficult to account for its use as a payment vehicle. As one technology investor put it, 'It's challenging if you have to think about capital gains before you buy a cup of coffee' (Rubin and Dougherty 2014).

Of course, every time the price of Bitcoin dropped and the mainstream media declared it dead – according to the feature 'Bitcoin Obituaries' on 99Bitcoins.com, Bitcoin has 'died' 179 times at time of writing – the most in the Bitcoin community, from miners to traders to mutualists alike, came out in support of its function as a payment system. Again and again, usually when prices are low, enthusiasts argue that 'the quote price of Bitcoin doesn't matter' or 'it's the payment system, stupid' (Irdial 2011, Hochstein 2013). The discursive flexibility between infrastructural mutualism and digital metallism perpetuates belief in Bitcoin when needed.

The cost of doing business?
The main exception to the tendency to hoard Bitcoins was on Silk Road, a website only accessible on the 'deep web' through the privacy-protecting encrypted web browser Tor. On Silk Road, Bitcoins could be used to buy

drugs and other illicit goods – often by people who had no other use for Bit-coins beyond that purpose (Chen 2011). Silk Road's built-in mechanisms allowed prices of goods and services to fluctuate with the Bitcoin exchange rate, with relatively little effect on sales. Some Silk Road vendors found that they could make more money simply by holding onto their Bitcoins than by accepting them. Indeed – when Silk Road first opened in 2011, Bitcoin was trading at $3, so if any vendors had held onto them for a year or more, they would have turned a healthy profit. For a time, Bitcoin speculation became more profitable than selling drugs.

It seemed that the only people who were willing to spend a currency that could double in price the next day were either drug addicts or recreational users who considered the potential for price fluctuation to simply be part of the cost of doing occasional business with a drug dealer (Greenberg 2013). Speculation made it impossible for anyone but the most desperate or dilettantish to use Bitcoin for payments. This undermined the infrastructural mutualist hope for privacy in everyday transactions.

The relationship between Silk Road vendors and Bitcoin speculators seemed to be symbiotic. According to testimony from Russ Ulbritch, the operator of the site, from February 2011 to July 2013, the total revenue generated from these sales was 9,519,664 Bitcoins, and the total commissions collected by Silk Road from the sales amounted to 614,305 Bitcoins, approximately equivalent to $1.2 billion in revenue and $79.8 million in commissions, at then-current Bitcoin (Fernholz 2013). After Silk Road was raided in 2013, the price of Bitcoin dropped 20 percent in three hours before eventually recovering (Tsjeng 2013).

For digital metallists, Bitcoin's high and volatile price need not be at odds with its ability to function as a payment. Many imagined that Bitcoin would function as niche currency that circulated alongside others. In the future, they argued, there would be enough special purpose currencies for every kind of payment, some of which 'cost' more to use and, eventually, there would be more sophisticated markets to seamlessly work out the differences between the prices of various currencies. This everyday competition in money was, itself, aligned with digital metallism. If some people made money off drug users' limited rationality, all the better.

The future: Vampire Squid and the Chthulucene

Bitcoin emerged from a technological, social, and economic context marked by undermined trust in existing institutions. With the rise of surveillant platform business models and the global financial crisis, Bitcoin was a way to obviate the need for authorities and 'middle men' of all kinds. Bitcoin drew from a longer history of cypherpunk and crypto-anarchy to perform two seemingly complementary but ultimately incompatible techno-economic

imaginaries: digital metallism and infrastructural mutualism. As these imaginaries were expressed in digital material infrastructures, it became clear that digital metallism undermined and overwhelmed infrastructural mutualism. As Brett Scott (2014) describes this tension:

> The vision thus is not one of bands of people getting together into mutualistic self-help groups. Rather, it is one of individuals acting as autonomous agents, operating via the hardcoded rules with other autonomous agents, thereby avoiding those who seek to harm their interests.

As a conclusion, I will turn to the future. Bitcoin, like all money, is speculative. It creates a shared present that projects a shared future. This article has examined the specific pasts – the legacies of the cypherpunks and crypto-anarchists – that Bitcoin pulls into the present. What range of possible futures does the present make available? In mythology, dragons and other monsters guard hordes of gold. In *Dungeons and Dragons* (a mythological system familiar to many Bitcoin enthusiasts) at least, monsters themselves have no use for gold, but they feed off of the belief energy with which humanoids imbue gold. What sort of dragons guard Bitcoin and feed off of belief in its speculative futures? In the following sections, I will draw from two monstrous visions: the *Vampire Squid* and the *Chthulucene*.

The Vampire Squid

After years of talking past each other, internecine sniping, and forked code, some in the Bitcoin community have, perhaps, begun to realize that the differences between the techno-economic imaginaries of infrastructural mutualism and digital metallism may be irreconcilable. Others continue to see their own version of the future in Bitcoin. The whole time, though, another, far more powerful techno-economic imaginary was ever-present in the background: global capitalism.

Beginning in earnest in 2015, most of the interest in Bitcoin has not been in its digital metallist capacity to serve as a speculative commodity. Instead, entrepreneurs and investors have been interested in Bitcoin's underlying ledger protocol, the blockchain. As the cover of *Bloomberg Markets* proclaimed, 'IT'S ALL ABOUT THE BLOCKCHAIN' (Robinson and Leising 2015). This new wave of innovation and investment is attempting to disentangle the blockchain mechanism from the Bitcoin economy. In Swartz (2017), I characterize these projects as 'incorporative' blockchain projects.

Around the same time that Bitcoin was first popularized, the Occupy movement took up as its mascot antagonist the 'vampire squid' (Roose 2011). As *Rolling Stone* writer Matt Taibbi described it in 2010, the global financial system was 'a great vampire squid wrapped around the face of humanity, relentlessly jamming its blood funnel into anything that smells like money'. And, indeed, Bitcoin may or may not be money, but it certainly smells like money.

While there are some blockchain projects that, like Bitcoin before them, attempt to produce radical social change, many are being developed from within the existing financial system. For example, a private blockchain could be used by a large bank to complete internal settlement between siloed areas of the bank, without incurring the costly fees currently associated with payment. Market makers could form an association to maintain the blockchain as their cost of entry to the market. This use of the protocol is less like the open World Wide Web and more like the global distribution system or GDS, which allows all airlines, travel agencies, and distribution channels to manage reservations and schedules in a single private network.

This would, in fact, be a kind of infrastructural mutualism, with the 'peers' supporting the shared platform as financial institutions, not individuals. As Diego Viana (2016) has pointed out, there are parallels between the technological arms race in mainstream finance and in the mining of Bitcoin. Hardin and Rottinghaus (2015) describe the ways in which financial technology does not merely coordinate markets, as others in the Social Studies of Finance have argued; rather, its enables profit-making practices, in particular arbitrage, in which profits are handed to the winners of these technological arms races. Embracing Bitcoin's blockchain technology is means for mainstream financial institutions to level-up, to have the most robust arsenal on the field, even if they do not yet know the nature of the battle. Dodd (2017, p. 3) identifies this paradox of Bitcoin's future: 'Bitcoin will succeed as *money* to the extent that it fails as an *ideology*.' Perhaps ironically, this seems to be the most likely way for the infrastructural mutualism dreamt of by early Bitcoin enthusiasts to linger on: for it to disappear into the vast, preserving, and multi-tentacled beast known as the global financial system.

The Chthulucene

And, yet perhaps a different future looms. With the rise of the authoritarian, ethno-nationalist so-called 'alt-right' (to which more than few of the most right-wing digital metallists have defected) across the globe, the compact between states and neo-liberal capitalism seems suddenly fragile. In the world's most powerful and wealthy nations, institutions are becoming enfeebled as state power is maximizing. Total coercive surveillance and failed currency may soon be more than the stuff of critical theory and crises 'elsewhere'. The apocalyptic future of totalitarianism and chaos that Bitcoin advocates of all stripes have always seen coming seems like it might indeed be well on its way.

Until then, a particular temporality has become a new normal. Anthropologist Jane Guyer (2007) suggests that, for some time now, public culture has become concerned only with responses to immediate situations and plans for far off futures. She traces this temporality to both an evangelical sense of prophecy and macroeconomic theories of growth. Bitcoin aficionados, many of

whom have taken up macroeconomic theory with near-religiosity, have been living in this 'evacuation of the near future' for some time (Guyer 2007, p. 409). They have been concerned with a self-prophesied apocalyptic rupture, when, perhaps, either the mutualist infrastructure will be called into service or their investments in digital metal will pay off. Indeed, two leaders in Bitcoin explained to me at a financial technology event in October 2017 that Bitcoin was like 'property'. It is a stake in a landscape that is only now emerging. Despite the on-going crisis of governance that rendered the underlying infrastructure unstable, by November, Bitcoin was trading at a then-all-time-high of nearly $7900 U.S. Dollars (Field 2017). It seems, in 2017, hard to know which rules, political, social, or economic, still apply.

As Zimmer (2017, p. 315) points out, there was always an apocalyptic logic of extraction to Bitcoin's digital metallism: 'we'll see the techno-utopianism surrounding this global digital currency dissolve into a dystopian realm of scarcity and misery, buried deep within the infernal depths of the earth'. Indeed, metallism is fundamentally geological, as is its temporality. As Zimmer (2017, p. 329) writes, 'Mining is always a terraforming operation. It reshapes the earth and its inhabitants in a profound way, one that resonates on the geological time scale.' The future is being terraformed and simultaneously exploited for extractable resources. Extraction, both of minerals and of informational processes, also involved what Mezzandro and Neilson (2017, p. 188) call the 'scrambling of time': expected temporal logics become unmoored like coal seams fracked into a slickwater slurry.

Perhaps we will see radical reorganization: digital fiefdoms lead by digital warlords who have been hoarding digital gold. Things might even be weirder than that. We may be at the inflection point of what Donna Haraway (2015) calls the 'the Chthulucene'. It is the world that comes after: after the damage that humans have done becomes truly cataclysmic. The term 'Chthulucene' draws from the ancient dread monster in the misogynist, racist nightmare world of H.P. Lovecraft. But Haraway (2015, p. 160) appropriates this tentacle-beast to imagine another way of being: becoming part of an assemblage of creatures that live among the compost of a dying world. She writes that we must now work to 'make kin': 'One way to live and die well as mortal critters in the Chthulucene is to join forces to reconstitute refuges, to make possible partial and robust biological-cultural-political-technological recuperation and recomposition, which must include mourning irreversible losses.'

Indeed, some newer blockchain-based projects aim to create new worlds, new ways of being together, using this technology. 'They use the imagery of fractals, swarms, and other formations that are deeply alter to the economy as it has usually been imagined.' In Swartz (2017), I detail what I call 'radical' blockchain projects and offer the critique that perhaps the slower temporality of incorporative blockchain projects might, ironically, surface the relational labour and therefore politics of infrastructure more than do the radical

projects. In many cases, these speculative visions are extensions of infrastructural mutualism. Can we imagine a new infrastructural mutualism in which 'peer to peer' means 'kin to kin'? In which the alterity of collective privacy is an act of taking refuge in the whale fall – that is, the carcass of a cetacean that supports a complex localized ecosystem that supplies sustenance to deep-sea organisms for as long as decades – of neo-liberal capitalism?

Bitcoin may not have gone mainstream, but its structure of feeling has. As Guyer puts it, many of us now feel like we have been living in a 'parenthetical period' between cataclysms. And now the closing parenthesis is becoming overburdened like a breached levy. The waters are pouring over. The distant future has been summoned into the near future. It is the future Bitcoin advocates warned against, and the future they conjured. Which future will it be: digital metallist or infrastructural mutualist?

Notes

1. In his forthcoming book, Finn Brunton gives a much more detailed history of the pursuit of digital cash than I convey here. I am heavily in dialogue here with Brunton, and my arguments are not incompatible with his, but I urge interested readers to consult his book for a sense of historical complexity and accuracy. I offer here a condensed history that simplifies a range of subject positions in an artificial distinction between cypherpunk and crypto-anarchy. These ideal types allow me to illuminate the distinction between *infrastructural mutualism* and *digital metallism* that, I argue, troubles the core of Bitcoin.
2. See May 1993 in the reference list. But also note that a compressed archive of the mailing list is available: https://www.mail-archive.com/cypherpunks@cpunks.org/msg00616.html [Accessed 11 November 2017].
3. I have chosen to follow the lead of most in the Bitcoin community and refer to Satoshi Nakamoto as 'Satoshi'. Works by Satatoshi Nakamoto will are found under Nakamoto (2008, 2009, 2015).
4. I make this assertion based on countless conversations with Bitcoin enthusiasts and professionals over the years who have read the original piece and have taken up 'digital metallist' as a political formation, although they frequently disagree with our critique of the position. For example, see Vigna and Casey (2016, p. 40) and the 2013 Bitcoin Forum post, *A Philosophy of Bitcoin – Do We Need One? YES!* (*Metallism, semiotics, and more*).
5. For a full transcript, see *Transcript of secret meeting between Julian Assange and Google CEO Eric Schmidt*, 2013.
6. See Rapid consolidation of Bitcoin mining pool operators, 2013.

Acknowledgements

Studies department at the University of Virginia, and the editors and anonymous reviewers of *Cultural Studies*.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Lana Swartz is an assistant professor of Media Studies at the University of Virginia. She is the co-editor of *Paid: tales of dongles, checks, and other money stuff* (MIT 2017).

References

2009 Exchange Rate [online], 2009. New liberty standard. Available from: http://newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate [Accessed 11 November 2017].

Antonopoulos, A., 2015. *Mastering Bitcoin*. Sebastopol, CA: O'Reilly Media.

Allen, J. and Pryke, M., 1999. Money cultures after Georg Simmel: mobility movement, and identity. *Environment and planning D: society and space*, 17 (1), 51–68.

Benkler, Y., 2011. A free irresponsible press: wikileaks and the battle over the soul of the networked fourth estate. *Harvard civil rights – civil liberties law review*, 46 (2), 311–397.

The Bitcoin Manifesto. 2011. *Bitcoin forum* [online]. Available from: https://Bitcointalk.org/index.php?topic=5671.0 [Accessed 11 November 2017].

Bitcoin Obituaries [online]. 99Bitcoins. Available from: https://99Bitcoins.com/Bitcoinobituaries/ [Accessed 11 November 2017].

Bitcoin Price. Coinbase [online]. Available from: https://www.coinbase.com/charts;%20http://www.coindesk.com/price/ [Accessed 11 November 2017].

BitStamp (USD), 2017. *Bitcoin charts* [online]. Available from: http://Bitcoincharts.com/charts/bitstampUSD#rg60ztgSzm1g10zm2g25zv [Accessed 11 November 2017].

Bjerg, O., 2015. How is Bitcoin money? *Theory, culture, and society*, 33 (1), 53–72.

Blanchette, J.-F., 2012. *Burdens of proof: cryptographic culture and evidence law in the age of electronic documents*. London: MIT Press.

Bradbury, D., 2014. *Can hobbyist Bitcoin miners still make a buck?* [online]. CoinDesk. Available from: http://www.coindesk.com/can-hobbyist-Bitcoin-miners-still-make-buck/ [Accessed 11 November 2017].

Brunton, F., 2017. *The Bank of England as a Ruin: Currency as communication of the future*. International Communication Association meeting, 28 May, San Diego, CA.

Carey, J.W., 1989. *A cultural approach to communication*. New York: Routledge.

Cawrey, D., 2014. *What are Bitcoin nodes and why do we need them?* [online]. Coindesk. Available from: http://www.coindesk.com/Bitcoin-nodes-need/ [Accessed 11 November 2017].

Chaum, D., 1985. Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, 28 (10), 1030–1044.

Chen, A., 2011. *Underground website lets you buy any drug imaginable* [online]. Wired. Available from: https://www.wired.com/2011/06/silkroad-2/ [Accessed 11 November 2017].

Dai, W., 1998. *B-Money* [online]. Available from: http://www.weidai.com/bmoney.txt [Accessed 11 November 2017].

Davidson, J., 2015. *No, big companies aren't really accepting Bitcoin* [online]. *Time*. Available from: http://time.com/money/3658361/dell-microsoft-expedia-Bitcoin/ [Accessed 11 November 2017].

De Filippi, P. and Loveluck, B., 2016. The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. *Internet policy review*, 5 (3), 1–28.

Desan, C., 2014. *Making money: coin, currency and the coming of capitalism*. Cambridge, MA: Harvard University Press.

Dillet, R., 2013. *Bitcoin Ticker available on bloomberg terminal for employees* [online]. Tech Crunch. Available from: https://techcrunch.com/2013/08/09/Bitcoin-ticker-available-on-bloomberg-terminal/.

Dodd, N., 1994. *The sociology of money*. Cambridge, MA: Polity Press.

Dodd, N., 2014. *The social life of money*. Princeton, NJ: Princeton University Press.

Dodd, N., 2017. The social life of Bitcoin. *Theory, culture & society* [online]. doi:10.1177/0263276417746464.

Fernholz, T., 2013. *Silk Road collected 9.5 million Bitcoin – and only 11.75 million exist*. *Quartz* [online]. Available from: https://qz.com/131084/silk-road-collected-9-5-million-bitcoin-and-only-11-75-million-exist/ [Accessed 11 November 2017].

Ferry, E., 2016. On Not being a sign: gold's semiotic claims. *Signs and society*, 4 (1), 57–79.

Field, M. 2017. *Bitcoin hits all time high as controversial 'hard fork' called off* [online]. *Telegraph*. Available from: http://www.telegraph.co.uk/technology/2017/11/09/bitcoin-hits-time-high-controversial-hard-fork-called [Accessed 11 November 2017].

Finney, H., 2008. *Re: Bitcoin P2P e-cash paper.* Cryptography Mailing list [online]. Available from: http://satoshi.nakamotoinstitute.org/emails/cryptography/12/. [Accessed 11 November 2017].

Franco, E., 2015. *Inside the Chinese Bitcoin Mine That's Grossing $1.5M a Month* [online]. Vice. Available from: https://motherboard.vice.com/en_us/article/chinas-biggest-secret-Bitcoin-mine [Accessed 11 November 2017].

Frissell, D., 1996 [2001]. Re: denning's crypto anarchy. Reprinted in P. Ludlow, ed., *Crypto anarchy, cyberstates, and pirate utopias*. Cambridge: MIT Press, 105–114.

Full Bitcoin Nodes [online], 2014. Available from: http://counterparty.io/news/full-Bitcoin-nodes/ [Accessed 11 November 2017].

Golumbia, D., 2016. *The politics of Bitcoin: software as right-wing extremism*. Minneapolis: University of Minnesota Press.

Graeber, D., 2001. *Toward an anthropological theory of value: the false coin of our own dreams*. New York: Palgrave Macmillan.

Graeber, D., 2011. *Debt: the first 5,000 years*. Brooklyn, NY: Melville House.

Greenberg, A., 2013. *Founder of drug site Silk Road says Bitcoin booms and busts won't kill his black market* [online]. *Forbes*. Available from: https://www.forbes.com/sites/andygreenberg/2013/04/16/founder-of-drug-site-silk-road-says-bitcoin-booms-and-busts-wont-kill-his-black-market/.

Guyer, J., 2007. Prophecy and the near future: thoughts on macroeconomic, evangelical, and punctuated time. *Journal of the American ethnological society*, 34 (3), 409–421.

Haraway, D., 2015. Anthropocene, capitalocene, plantationocene, chthulucene: making Kin. *Environmental humanities*, 6. 159–165.

Hardin, C. and Rottinghaus, R., 2015. Introducing a cultural approach to technology in financial markets. *Journal of cultural economy*, 8 (5), 547–563.

Hart, K., 1986. Heads or tails? Two sides of the coin. *Man*, 21 (4), 637–656.

Hart, K., 2001. *Money in an unequal world: Keith Hart and his memory bank*. New York: Texere.

Hochstein, M., 2013. Why Bitcoin matters: it's the payment system, Stupid! [online]. *American Banker*. Available from: https://www.americanbanker.com/morning-scan/why-bitcoin-matters-its-the-payment-system-stupid [Accessed 11 November 2017].

Hudson, M., 2004. The archaeology of money: debt versus barter theories of money's origins. *In*: L.R. Wray, ed., *Credit and state theories of money: the contributions of A. Mitchell Innes*. Cheltenham: Edward Elgar, 99–127.

Hughes, E., 1993. *A Cypherpunk's manifesto* [online]. Available from: https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto [Accessed 11 November 2017].

Ingham, G., 1996. Money is a social relation. *Review of social economy*, 54 (4), 507–529.

Ingham, G., 2004. *The nature of money*. Cambridge: Polity Press.

Irdial, 2011. *Why the quoted price of Bitcoin doesn't matter* [online]. BlogDial. Available from: http://irdial.com/blogdial/?p=3207 [Accessed 11 November 2017].

IRS virtual currency guidance: virtual currency is treated as property for U.S. federal tax purposes; General rules for property transactions apply [online], 2014. Available from: https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance [Accessed 11 November 2017].

Jeong, S., 2013. *The Bitcoin protocol as law, and the politics of a stateless currency*. Available from: https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2294124 [Accessed 11 November 2017].

Kahn, D., 1967. *The codebreakers: the comprehensive history of secret communication from ancient times to the internet*. New York: Scribner.

Karlstrøm, H., 2014. Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: journal of social theory*, 15 (1), 23–36.

Levy, S., 2001. *Crypto: how the code rebels beat the government – saving privacy in the digital age*. New York: Penguin Group.

Maurer, B., 2005. *Mutual life, limited: Islamic banking, alternative currencies, lateral reasoning*. Princeton, NJ: Princeton University Press.

Maurer, B., Nelms, T., and Swartz, L., 2013. When perhaps the real problem is money itself! The practical materiality of Bitcoin. *Social semiotics*, 23 (2), 261–277.

May, T., 1992. *The crypto-anarchy manifesto* [online]. Available from: http://www.activism.net/cypherpunk/crypto-anarchy.html [Accessed 11 November 2017].

May T., 1993. *The crypto-anarchist manifesto* [online]. Available from: http://www.alamut.com/subj/ideologies/manifestos/cryptoanarchist.html.

May, T., 1994. *The Cyphernomicon* [online]. Available from: https://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.txt [Accessed 11 November 2017].

May, T., 1996. *Untraceable digital cash, information markets, and BlackNet* [online]. Available from: http://osaka.law.miami.edu/~froomkin/articles/tcmay.htm [Accessed 11 November 2017].

McMillan, R., 2013. *Inside the race to build the world's fastest Bitcoin Miner* [online]. Wired. Available from: http://www.wired.com/2013/04/Bitcoin-mining-rigs/ [Accessed 11 November 2017].

Mezzandro, S. and Neilson, B. 2017. On the multiple frontiers of extraction: excavating contemporary capitalism. *Cultural studies*, 31 (2–3), 185–204.

Modem Grrrl. 1995. *Wired* [online]. Available from: https://www.wired.com/1995/02/st-jude [Accessed 11 November 2017].

Nakamoto, S., 2008. *Bitcoin: a peer-to-peer electronic cash system* [online]. Available from: https://bitcoin.org/bitcoin.pdf [Accessed 11 November 2017].

Nakamoto, S., 2009. *Bitcoin open source implementation of P2P currency* [online]. Available from: http://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/ [Accessed 11 November 2017].

Nakamoto, S., 10 Dec 2015. [Bitcoin-dev] not this again. *The Linux Foundation* [online]. Available from: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-December/011936.html [Accessed 11 November 2017].

Narayanan, A., 2013. What happened to the crypto dream? Part 1. *IEEE security & privacy*, 11 (2), 75–76.

Peck, M., 2017. *Why the biggest Bitcoin Mines are in China*. IEEE spectrum. Available from: https://spectrum.ieee.org/computing/networks/why-the-biggest-bitcoin-mines-are-in-china [Accessed 11 November 2017].

Popper, N., 2013. *Into the Bitcoin Mines* [online]. *New York Times*. Available from: http://dealbook.nytimes.com/2013/12/21/into-the-Bitcoin-mines/?_php=true&_type=blogs&_r=1 [Accessed 11 November 2017].

Popper, N., 2015. *Digital gold: Bitcoin and the inside story of the misfits and millionaires trying to reinvent money*. New York: Harper Collins.

Popper, N. and Lattman, P., 2013. *Never mind Facebook; Winklevoss twins rule in digital money* [online]. *The New York Times*. Available from: https://dealbook.nytimes.com/2013/04/11/as-big-investors-emerge-Bitcoin-gets-ready-for-its-close-up/ [Accessed 11 November 2017].

A philosophy of Bitcoin – do we need one? YES! (Metallism, semiotics, and more) 2013 [online]. Bitcoin Forum. Available from: https://bitcointalk.org/index.php?topic=230416.0 [Accessed 11 November 2017].

Rafferty, M. and Bryan, D., 2006. Financial derivatives: the new gold? *Competition & change*, 10 (3), 265–282.

Rapid consolidation of Bitcoin mining pool operators [online], 2013. Hacker News. Available from: https://news.ycombinator.com/item?id=6894320 [Accessed 11 November 2017].

Reitman, R., 2011. *Bitcoin – a step toward censorship-resistant digital currency* [online]. Available from: https://www.eff.org/deeplinks/2011/01/Bitcoin-step-toward-censorship-resistant [Accessed 11 November 2017].

Robinson, E. and Leising, M., 2015. *Blythe masters tells banks the blockchain changes everything* [online]. Available from: https://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything [Accessed 11 November 2017].

Rodger, W., 2001. *R.I.P. Cypherpunks* [online]. SecurityFocus. Available from: http://www.securityfocus.com/news/294 [Accessed 11 November 2017].

Roose, K., 2011. *The long life of the vampire squid* [online]. *The New York Times*. Available from: https://dealbook.nytimes.com/2011/12/13/the-long-life-of-the-vampire-squid-metaphor/ [Accessed 11 November 2017].

Rubin, R. and Dougherty, C., 2014. *Bitcoin currency use impeded by IRS property treatment* [online]. Ganer+Ganer. Available from: http://www.ganer.com/blog/2014/march/Bitcoin-currency-use-impeded-by-irs-property-tre.aspx [Accessed 11 November 2017].

Russell, A. and Vinsel, L., 2016. *Hail the maintainers* [online]. Aeon. Available from: https://aeon.co/essays/innovation-is-overvalued-maintenance-often-matters-more [Accessed 11 November 2017].

Schneider, N., 2015. *After the Bitcoin Gold Rush* [online]. New Republic. Available from: https://newrepublic.com/article/121089/how-small-Bitcoin-miners-lose-crypto-currency-boom-bust-cycle [Accessed 11 November 2017].

Scott, Brett, 2014. *Visions of a techno-Leviathan: the politics of the Bitcoin Blockchain* [online]. E-International Relations. Available from: http://www.e-ir.info/2014/06/01/visions-of-a-techno-leviathan-the-politics-of-the-bitcoin-blockchain/ [Accessed 11 November 2017].

Swartz, L., 2017. Blockchain dreams: imagining techno-economic alternatives after Bitcoin. *In*: M. Castells, ed., *Another economy is possible*. Cambridge: Polity Press, 82–105.

Szabo, N., 2011. *Bitcoin, what took ye so long?* [online]. Available from: http://www.unenumerated.blogspot.com/2011/05/bitcoin-what-took-ye-so-long.html [Accessed 11 November 2017].

Taibbi, M., 2010. *The Great American bubble machine* [online]. Rolling Stone. Available from: http://www.rollingstone.com/politics/news/the-great-american-bubble-machine-20100405 [Accessed 11 November 2017].

Thought experiment: is Bitcoin a Ponzi? [online], 2011. Available from: https://Bitcointalk.org/index.php?topic=4259. [Accessed 11 November 2017].

Transcript of secret meeting between Julian Assange and Google CEO Eric Schmidt [online], 2013. Wikileaks. Available from: https://wikileaks.org/Transcript-Meeting-Assange-Schmidt.html. [Accessed 11 November 2017].

Tsjeng, Z., 2013. *Silk Road conspiracy theories* [online]. Dazed Digital. Available from: http://www.dazeddigital.com/artsandculture/article/17454/1/silk-road-conspiracy-theories [Accessed 11 November 2017].

Viana, D., 2016. Two Technical Images: Blockchain and High-Frequency Trading. *Philosophy and technology*, 1–26.

Vigna, P. and Casey, M., 2016. *The age of cryptocurrency*. New York: St. Martin's Press.

Re: Wikileaks contact info? [online], 2010. BitcoinTalk. Available from: https://bitcointalk.org/index.php?topic=1735.150 [Accessed 11 November 2017].

World's First Mining Pool, 2010. *Bitcoin forum* [online]. Available from: https://Bitcointalk.org/index.php?topic=1976.0 [Accessed 11 November 2017].

Zimmer, Z., 2017. Bitcoin and Potosí silver historical perspectives on cryptocurrency. *Technology and culture*, 58 (2), 307–334.