Article

Theory Culture & Society

Theory, Culture & Society
2019, Vol. 36(4) 49–72

DOI: 10.1177/0263276419826218
journals.sagepub.com/home/tcs

SAGE

The Socio-Technological Lives of Bitcoin

Adam Hayes
University of Wisconsin-Madison

Abstract

Bitcoin, cryptocurrencies, and blockchains have become buzzwords in the media and are attracting increasing academic interest, mainly from the fields of computer science and financial economics. In this essay, I argue that cryptocurrencies and blockchains are important objects of general social science research and thought, but not for their 'moneyness' per se. Through a historical sociology of the antecedents and discourse leading up to Bitcoin, I show that it was never meant to be 'money' in the economic sense, but rather a solution to a technical puzzle for preventing opportunistic actors from double-spending digital 'coins,' as well as a fervent ideology surrounding online privacy and infringement of individual rights in the digital age. Drawing from themes in science and technology studies, I suggest that Bitcoin and other 'cryptoassets' are properly socio-technological assemblages that constitute new and important objects of social inquiry that must be understood beyond the myopic context of crypto-money. I conclude by proposing three alternative ontologies for blockchains relevant to economic, political, and social life: as systems of accounting, as organizational forms, and as institutions in their own right.

Keywords

assemblages, Bitcoin, blockchain, economy, money, technology

Introduction

> The foundation is being laid for a dossier society, in which computers could be used to infer individuals' life-styles, habits, whereabouts, and associations from data collected in ordinary consumer transactions. Uncertainty about whether data will remain secure against abuse by those maintaining or tapping it can have a 'chilling effect.' (David Chaum)

Bitcoin, cryptocurrencies, and blockchains have become buzzwords in the media and are attracting increasing academic interest, mainly from

Corresponding author: Adam Hayes. Email: ahayes8@wisc.edu
Extra material: http://theoryculturesociety.org/

the fields of computer science and financial economics.[1] However, its status as a compelling object of research more broadly in the social sciences has remained elusive. Recently, this gap has begun to be filled. For instance, Hendrickson et al. (2016) and Tasca et al. (2018) explore the political economy internal to the Bitcoin system, while Golumbia (2016) interrogates Bitcoin's software as a form of political action through bypassing banks for the creation of money, and Maurer (2017) examines how bitcoins are variously earmarked by those transacting with it. But, in filling this gap, another gap appears. For to consider Bitcoin as a new money-form *par excellence* risks generating a myopic understanding of its sociological importance (as well as that of its underlying technology, known generically as *the blockchain*). Further, such a definite understanding obscures and blackboxes Bitcoin's pre-history by making the tacit supposition that being a crypto-*currency* had been teleological. If one concentrates on issues concerning the 'moneyness' of cryptocurrencies one is in danger of overlooking the main sociological significance.

Nigel Dodd (2014, 2018) brings Bitcoin into focus as an important object of sociological inquiry by understanding it broadly as a social movement – as a contested social space – thus challenging the notion that Bitcoin is trust-free money (but see also Bjerg, 2016; Nelms et al., 2018). Dodd (2018: 35) sets out by citing what seems to be an apparent paradox: 'if Bitcoin succeeds in its own terms as an *ideology*, it will fail in practical terms as a form of *money*.' I no doubt agree with this point, yet it once again confines our analysis by drawing a dichotomy that rests on the assumption that Bitcoin is meant to be equivalent to *money* in the first place. Dodd reasons that if Bitcoin operates as a mere monetary automaton, then it obscures the social forces and grassroots movements that construct and reconstruct it, writing that 'the idea behind Bitcoin is premised on denying what I believe is Simmel's most important insight into the social life of money: by treating money as a *thing*, not a *process*' (2018: 51). I build on this sentiment by arguing that there are imperative technical and social processes of Bitcoin that transcend its status *qua* money. Drawing from science and technology studies, I suggest that Bitcoin and other 'cryptoassets' are properly socio-technological assemblages (Callon, 1998; Latour, 2005) that enroll both human and non-human elements, and which are indeed of sociological interest, but not because they operate as money per se. Rather, it is what these assemblages are able to accomplish: they bring people together directly through the radical disintermediation of institutions, which are in turn superseded by a technological locum. By 'radically disintermediate,' I mean that Bitcoin and its descendants enable purely peer-to-peer transfers of (e.g.) property rights *without the need for a trusted third party* to ensure a credible commitment. The implications are indeed significant. As a case in point, it is commonly held that one of the critical roles of the state is to enforce property rights (Besley and Persson, 2009). Enforcement by the

state is posited to reduce self-enforcement costs, which increases the value of assets and incentivizes economic growth and prosperity (Alston and Mueller, 2008). Even in the most minimalist libertarian versions of a 'night-watchman state,' one of the goals of the government is still to enforce property rights (Titmuss, 1974). The very existence of Bitcoin and other blockchain-based networks along with their global adoption evokes the possibility for the governmentality of algorithms on society.

The interpretation of Bitcoin that the fundamental trust embedded in money has simply been transposed into 'machine code' while severing all ties with social relations is thus misplaced. Machine code has not *replaced* social relations; it has been joined together with them. In fact, by engendering true peer-to-peer interactions Bitcoin and other blockchains foster *more direct* personal connections, however mediated by technology, while sidestepping the conventional web of indirect relations between and among individuals, firms, institutions, and governing bodies. Whether Bitcoin (or some other cryptocurrency) will succeed or fail at being money is consequently the wrong question to ask. The imperatives are instead existential: what *is* Bitcoin (and blockchain) and how does it structure social interaction? I begin my inquiry by looking to the past – by mapping the antecedents of Bitcoin using an analysis of archived online discussion forums, personal web pages, blog posts, and email exchanges of important actors, as well as from a literature review of key developments found in academically applied cryptography from the 1980s and 1990s. I seek to elaborate on these in order to show that Bitcoin was not meant to be a prototypical internet money *par excellence*, but rather a particular tool-set to enable peer-to-peer transfers of private property rights – where monetary instruments were but one possibility. Looking at the historical sociology of what would become Bitcoin, it becomes clear that being a 'good money' (in the economics sense) was not an ongoing concern. In fact, those most influential to the Bitcoin project publicly conjectured that a cryptocurrency would be more akin to a collectible or a commodity than money. The primary drivers in Bitcoin's development were thus patently non-economic and instead comprised: (1) the technical puzzle of preventing opportunistic actors from *double-spending* digital 'coins' and (2) an ideology of online privacy in the digital age.

The first section of this paper traces the development of the necessary pieces that will come together to ultimately create Bitcoin. These pieces are technological artifacts in the form of inscriptions: theory, formulas, design elements, and lines of computer code. These pieces, moreover, come to be loaded with symbolic meaning based on a worldview where computerization creates vulnerabilities and concerns over surveillance of individuals by corporate or state actors. In the second section, I propose alternative ontologies for understanding what Bitcoin is by abstracting

from it the underlying socio-technological assemblage that is the blockchain. More than diverse social perspectives or interpretations of blockchains in society, different configurations and practices come to perform blockchains as different and distinct entities. I propose that blockchains can be enacted variously as systems of accounting, as organizational forms, and as institutions in their own right.

Trust in the System

Chancellor on Brink of Second Bailout for Banks

On 3 January 2009, the very first block of bitcoins was created. Embedded in that 'genesis block' was the following text: *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*, referring to an actual *Financial Times* headline about the deepening economic crisis.[2] Indeed, those inserted words suggest that the timing of Bitcoin's release concurrent with the erosion of trust in financial institutions appears to have been opportunistic. What better time to interrogate the removal of a trusted third party than when that third party is no longer trusted? Yet, as I will show, Bitcoin did not appear suddenly and fully formed. It resulted from an ongoing process of enlisting technological advances with social and political forces.

In 2008, global financial markets crashed and much of the world entered a prolonged economic recession. On 31 October 2008, a technical paper entitled 'Bitcoin: A Peer-to-Peer Electronic Cash System' appeared on the internet mailing list Cypherpunks, authored under the pseudonym Satoshi Nakamoto.[3] Nakamoto (2008) begins:

> A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution . . . based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

Nowhere in Nakamoto's nine-page proposal are any references to the moneyness of Bitcoin, how it might fulfil a store of value or unit of account, or how it might carry out monetary policy.

The true nature of money remains contested ground in the social sciences. Divergent schools of economic thought from the classical to the Austrian, from the neoclassical to the Marxist, each have their own particular theories of money. The anthropological and sociological traditions also have much to say on the nature of money, from Weber and Simmel to contemporary thinkers such as Bill Maurer and Viviana Zelizer. Standard-issue economics textbooks on money and banking (e.g. Mishkin, 2007: 53–5) suggest that 'whether money is shells or rocks or gold or paper, it has three primary functions in any economy: as a medium

of exchange, as a unit of account, and as a store of value. Of the three functions, its function as a medium of exchange is what distinguishes money from other assets such as stocks, bonds, and houses.'[4] Others, like Wray (1998), Ingham (2013) and Graeber (2012) argue that it is the social unit of account (or *numeraire*) function that is of prime importance. Without a socially recognized yardstick of equivalence, prices associated with exchange or values meant to be stored are unidentified and ambiguous. It is because we price stocks, bonds, and houses in money units and not in stock units that a dollar or euro is money and shares are not. Put differently, people come to a consensus on what the socially recognized money units are.

Beyond what money is or what functions it must serve, market economies also rely on some sort of monetary policy to regulate commerce and credit in response to fluctuations in the underlying economy. In modern times this has been the domain of the central banks; however, monetary authority has been present in some form dating to Medieval Europe (Broadberry and Gupta, 2006) and as far back as ancient China (Von Glahn, 1996). As for the actual 'monetary policy' for the Bitcoin system, it too seems distanced from prevailing notions of money, as well as quite arbitrary. Upon release of the first version of the Bitcoin software (v0.1), Nakamoto posted:

> Total circulation will be 21,000,000 coins. It'll be distributed to network nodes when they make blocks, with the amount cut in half every 4 years.
>
> first 4 years: 10,500,000 coins
>
> next 4 years: 5,250,000 coins
>
> next 4 years: 2,625,000 coins
>
> next 4 years: 1,312,500 coins etc. . . .
>
> When that runs out, the system can support transaction fees if needed. It's based on open market competition, and there will probably always be nodes willing to process transactions for free.[5]

The math implies that a block of bitcoins will be produced on average once every 10 minutes and that the last block will be mined around the year 2140.

The striking absence of monetary discourse leading up to Bitcoin is matched equally by the impressive bricolage of competing monetary principles that has attached itself to Bitcoin since its launch. The Cypherpunks, the group most directly responsible for the implementation of Bitcoin and who were among its earliest users, adhered to a strict form of

libertarianism informed by Austrian economics. Meanwhile, the fixed and deflationary monetary schedule described above is most closely associated with monetarist theories put forth by Milton Friedman and the Chicago School (see Selgin, 2015). Others, like Zimmer (2017) and Swartz (2018), find that some consider Bitcoin to be metallist in nature, like a virtual gold (cf. Maurer et al. 2013). At the same time, the actual price of bitcoins observed in the market (see Hayes, 2018) resembles a labor-cost theory of value advanced by the classical political economists.

Nevertheless, the point to be made here is not whether Bitcoin fails or succeeds at being money, but that these considerations are conspicuously absent from the discourse around its early development. Moreover, debates over whether or not Bitcoin is money (e.g. Yermack, 2015; Bjerg, 2016) are apt to take us down an intellectual rabbit hole that could prevent more generative discourse and theorizing. Instead, let us trace Bitcoin's history to see where it may lead.

Pecunium ex machina

Since the dawn of the computer age, creating a digital form of money had been both an intriguing and vexing idea. How can one prevent counterfeiting when money exists as binary data? How can one prove it is *they* who are in possession of a virtual 'coin'? How can such a money be securely stored and transferred between computers? How can anonymity be preserved in a system where digital traces are recorded all along the way? The true origin of cryptocurrencies does not begin with radical notions of uncoupling money from the state or disrupting central bank hegemony. Instead, it begins by seeking answers to practical questions like the ones above, provoked by fundamental puzzles about existence in cyberspace. Meanwhile, economic notions of what constitutes *moneyness* were absent or inchoate throughout.

In 1982, a group of academic mathematicians and computer scientists met for the second annual CRYPTO conference at the University of California at Santa Barbara. In attendance was a newly minted Berkeley PhD named David Chaum. There, he presented part of his dissertation thesis entitled 'Blind Signatures for Untraceable Payments' (Chaum, 1983), outlining how cryptography could theoretically be applied to create secure, anonymous digital payments – the first known reference to what will become a *cryptocurrency*.[6] Chaum's innovation was to use a pair of cryptographic 'keys,' one known publicly, coupled with a private key retained by its owner. The public key would function as an identifier much like a bank account number; the private key would be used as a 'blind' digital signature proving that the public key in fact belonged to the party in question while preserving anonymity.

Concerned with the implications of impending computerization, Chaum (1983: 199) was prescient: 'Automation of the way we pay for

goods and services is already underway . . . The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy.' Chaum, however, did not seek to disrupt the financial system; rather, he sought a way to protect consumers in the digital age by working with existing institutions. Chaum went on to start a private company called DigiCash in 1989 to realize the goal of protecting online transactions through cryptographically secured 'ecash,' aligning with commercial banks including Mercantile Bank in the US and Deutsche Bank in Germany.[7] The company, however, filed for bankruptcy in 2002 after failing to gain support from both end-users and financial backers. But, just like Mastercard, PayPal, or other e-payments rails, DigiCash was denominated in the users' domestic unit of account. DigiCash provided a secure way to transmit money through the internet, but that money would still be dollars, euros, or yen.

Throughout the 1980s and '90 s, the CRYPTO conferences continued to attract scholars who built on Chaum's groundbreaking idea. At CRYPTO '83, a trio of Israeli computer scientists introduced the concept of an 'electronic wallet,' designed to store 'unforgeable amounts of digital money' with the ability to transact between other such wallets using a 'public key cryptosystem' (Even et al., 1984). Cryptocurrencies are still held in what are colloquially known as wallets, based on this work.

Soon enough, a major technical hurdle came to be fully appreciated, which could undermine all of the theoretical developments made thus far: the so-called 'double-spend' problem. What is to prevent anyone from making several copies of an electronic coin and using them at different locations simultaneously? Chaum returned to CRYPTO '88 along with co-authors to propose a solution to this problem. Using additional cryptographic methods called *zero-knowledge proofs* (ZKPs) they could 'allow a bank to trace a repeat spender . . . so that the bank can supply incontestable proof that [she] has reused her money' (Chaum et al., 1988).

The significance of zero-knowledge proofs is that you can demonstrate the veracity of some fact *without knowing what the fact is*. The following example adapted from Quisquater et al. (1989: 628–30) illustrates the intuition behind a ZKP: Suppose your friend has discovered a magic codeword which unlocks an enchanted door located inside a ring-shaped cave.[8] Your friend refuses to tell you the magic word, making you suspicious of the authenticity of her claim. How can you confirm that she indeed knows this fact without knowing its contents? The cave has two forking paths, A & B, heading either left or right, which converge at the far end of the ring – where the magic door sits. Your friend enters the cave and takes either path at random without you seeing which way she went. You then shout into the cave and tell your friend from which path she should exit. If she indeed knows the magic word, she will consistently follow your instructions since she can unlock the door and

proceed around the ring. However, if she does not know the codeword there is still a 50 percent chance that she will exit from the correct path. Yet, by repeating this task many times the probability that she follows your directions by chance alone quickly approaches zero. Thus, you can conclude that she knows the magic word without knowing what it is. With this same logic, you can know if a digital coin has been double-spent without knowing anything about the spender.

At CRYPTO '89, a pair of Japanese researchers (Okamoto and Ohta, 1989) improved upon this zero-knowledge design and proposed a new type of electronic cash, which for the first time could be subdivided into many pieces. Four years later, it was shown how cryptographic protocols could be employed by an issuing bank to prevent double-spending of a digital coin *proactively* instead of detecting it after the fact (Brands, 1993). Each of these innovations was cumulative, building off an existing literature and following what Kuhn (1962) would call 'normal science.' For Kuhn, science advances incrementally within an established paradigm of knowledge-making, where members of a field share a recognition for key past achievements and for what puzzles are worth solving. Even for Chaum, advancing the idea of a cryptocurrency was built on years of previous research. The use of public and private key pairs, for instance, was adapted from pioneering work by Diffie and Hellman (1976), later iterated by Rivest, Shamir and Adleman (1978), where Chaum's contribution followed a logical progression as part of the same paradigm (see Narayanan and Clark, 2017, for more on Bitcoin's academic pedigree). By the 1990s, the use of cryptography effectively allowed for a virtual coin to be securely held and transferred anonymously between parties; however, the solution for double-spend still rested in some 'bank' or 'mint' to validate that a coin has not already been spent. The fidelity of the system ultimately boils down to trust in that third party.

Members of our society tend to trust the government, the banking system, the credit card operators, the law – to ensure that economic transactions and property rights are sound. Why then should we seek to disintermediate third parties and hand over the reins to some decentralized algorithm? The answer is an ideological one. As Dodd (2018) points out, the appeal to a disintermediated money has found favor among groups as disparate as libertarians and anarchists to hippies and computer geeks. While each of these groups may mistrust the government for one reason or another, I turn my attention to the Cypherpunks, whose members actively participated in the discourse around the creation of Bitcoin. The Cypherpunks, an influential group of thinkers, technologists, and software developers, picked up where solving the double-spend problem left off and valorized the groundwork laid above with an ideological practice.

In Crypto We Trust

Timothy May was an early engineer at Intel who solved some important technical issues around silicon chip fabrication, but he is best known for his active role in the online mailing list, the Cypherpunks, which appeared in the early 1990s, attracting as many as 700 subscribers at its peak.[9] May (1994) penned the Cypherpunk's original mission statement, arguing that the government should not be able to snoop into people's affairs; that protection of privacy is a basic right; that these rights must be secured through *technology* rather than through law; and that the power of technology often creates new political realities. Taken to its extreme, some members of the movement advocated for a *crypto-anarchy*, where governments and institutions are effectively replaced with technological solutions that ensure individual freedom, prosperity, and – above all – privacy.

The Cypherpunks also revered the work done by the academic cryptographers. One devotee of this research was Hal Finney, a computer scientist who helped develop the now-ubiquitous PGP encryption protocol. In a 1992 blog post, Finney writes:

> Here we are faced with the problems of loss of privacy, creeping computerization, massive databases, more centralization – and Chaum offers a completely different direction to go in, one which puts power into the hands of individuals rather than governments and corporations. The computer can be used as a tool to liberate and protect people, rather than to control them. Unlike the world of today, where people are more or less at the mercy of credit agencies, large corporations, and governments, Chaum's approach balances power between individuals and organizations.[10]

The first crypto-application that came out of the movement was an anonymous re-mailer, a server that receives email messages and then forwards them on to their intended recipient, removing any identifying information of the sender. On the surface this kind of application may seem esoteric, but it speaks volumes to the worldview shared by this group and the ideology embedded in their software. Finney (1992) continues:

> [Re-mailers] represent the 'ground floor' of this house of ideas – the ability to exchange messages privately, without revealing our true identities. In this way we can engage in transactions, show credentials, and make deals, without government or corporate databases tracking our every move as they can today. Only by securing the ability to communicate privately and anonymously can we take the

> next steps towards a world in which we each have true ownership and control over information about our lives.

In May of 1993, fellow Cypherpunk Nick Szabo similarly wrote:

> Most e-mail users are unaware that it is the most public medium ever invented, and use it to write love letters, letters to their lawyer, discussion of illegal activities, etc. Vast volumes of e-mail can be stored on small magnetic tapes and searched in bulk for keywords, e.g. 'mari[jh]uana'. The good news is, the computer brings an even greater weapon to fight these threats to our privacy and political freedoms: widely available, automatic cryptography.[11]

What is clear from these excerpts is a shared belief that the widespread use of information technology poses an existential threat since governments or other powerful actors can eavesdrop on private affairs. But, at the same time, it is also a technology that can be used to restore personal privacy.

One of the main ambitions, and indeed one of the recurring themes, of the Cypherpunks was to create a secure, digital 'cash' in order to ensure privacy of economic transactions and similarly prevent snooping from the government or corporations – a particular type of payment that could pass readily from one person to another without a bank or government agency facilitating it in any way. 'Privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system,' wrote Eric Hughes (1993), one of the Cypherpunk's co-founders and author of the group's manifesto. Cryptography provided the obvious technical solution to creating an anonymous payments system; however, the unit of account attached to such digital cash remained unspoken. In fact, throughout this discourse money appears to be conflated entirely with medium of exchange. The Cypherpunk manifesto is suggestive: 'When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am' (Hughes, 1993). The reconfiguration of that cash transaction from a piece of paper in hand to digital traces sent by computer does not change the fact that the nature of the 'cash' is granted exogenously (e.g. by the state as dollars) – just as anonymous re-mailers did not seek to create parallel email systems with their own protocols.

In the late 1990s, Nick Szabo began work on a new type of peer-to-peer exchange. Szabo was captivated by the concept of transferring property rights over encrypted computer networks. Of particular concern was the perceived ability of the state or other powerful actors, especially in times of political instability, to destroy or confiscate property such as homes and land or their corresponding records. Even in times of stability, property owners often feel the need (or are compelled) to purchase title

insurance to validate ownership. Szabo (1998a) proposed a solution based on combining the cryptographic methods developed in the 1980s

> with new advances in replicated database technology [that] will give us the ability to securely maintain and transfer ownership for a wide variety of kinds of property, including not only land but chattels, securities, and monetary instruments. This technology will give us public records which can 'survive a nuclear war' . . . While thugs can still take physical property by force, the continued existence of correct ownership records will remain a thorn in the side of usurping claimants.

This idea of a secure record of property rights enforced by a replicated database sows the seeds for what will become blockchain technology. A *blockchain* generically is a decentralized and public digital ledger that maintains every transaction in linear, chronological order reproduced across many computers such that records cannot be altered or deleted retroactively without the collusion of most nodes in the network. Szabo (1998a) continues:

> A group gets together on the Internet and decides to keep track of the ownership of some kind of property. This property is represented by 'titles': names referring to the property, and the public key corresponding to a private key held by its current owner, signed by the previous owner, along with a chain of previous such titles. The purpose of the replicated database is simply to securely agree on who owns what. The entire database is public.

In theory, the idea is persuasive. In practice, reaching group consensus that all entries in the ledger are valid is tricky. To illustrate this trickiness, consider the Byzantine Generals Problem (Lamport et al., 1982): Imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general, and where the generals can only communicate with one another by sending a messenger. After observing the enemy, they realize that their attack can only succeed if they are able to coordinate a common plan of action at an agreed upon time. However, some of the generals may be traitors. Moreover, it cannot be known that a messenger sent from one camp to another will not be intercepted by the enemy. Lamport and his colleagues prove (mathematically) that coordination can never be achieved under 'normal' conditions, since one can never be convinced that all are still loyal; however, consensus *can* nonetheless be realized given the right incentives and the existence of unforgeable messages based on cryptography.

For a replicated database, new entries must be confirmed in a way that is tolerant to the Byzantine Generals Problem, solved by a cryptographic trick known as 'proof-of-work.' Proof-of-work was first proposed as an answer to the growing problem of junk email in the early 1990s. At CRYPTO '92, Dwork and Naor (1993: 140–1) (who had worked with Chaum on ZKPs) proposed a scheme requiring the sender of an email to compute some moderately expensive but not intractable function in order to gain access to send, thus preventing frivolous use. The sender would have to present a valid proof that resources had been expended to get that permission. Such a proof function may take several seconds or minutes to solve, which would not be prohibitive in most cases, but would impose a substantial cost on a spammer. Jakobsson and Juels (1999) extended the proof-of-work model from junk email to ensuring the fidelity of an online micropayments system called MicroMint. It is this sort of proof-of-work that Szabo (1998b) also adopts for his replicated database. As proof-of-concept, he designed a peer-to-peer mechanism to transfer ownership rights to a virtual commodity named 'bit gold':

> [I]t 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. Bit gold. My proposal for bit gold is based on computing a string of bits from a string of challenge bits, using functions called 'proof of work functions' . . . The resulting string of bits is the proof of work.

The reframing of digital cash as a scarce virtual *commodity* also served a particular political purpose hostile to the perception of governments' unrestrained use of fiat currency as an 'inflationary weapon'. From this perspective, a decentralized, pro-privacy cryptocurrency should also be deflationary by design – to preserve its value based on scarcity, but also as an ideological statement. Swartz (2018: 9–10) defines this philosophy as *digital metallism*, where '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' – as a store of speculative value contingent on the collapse of the current social order.

Bit gold was never implemented, but it completed the circle (see also Wei Dai's (1998) 'b-money'). By the turn of the millennium, the ideological and technological pieces were in place for a decentralized cryptocurrency. Absent from this account is a coherent and sustained discussion of *money*, or how any particular theory of money would insert itself into a cryptocurrency. The Cypherpunks weren't economists, after all.[12] And, while the words 'cash', 'coin', and indeed 'money' were

invoked at times, they appear detached from a theoretical or conceptual hook. It remains striking that such little attention was paid to actual monetary economics or monetary policy.

On 10 January 2009, Satoshi Nakamoto sent 10 bitcoins to Hal Finney, marking its first transaction.[13]

What's Money Got to Do with It?

If an intellectual discourse around money was omitted in the pre-history of Bitcoin, how did its early contributors think about it? 'It occurs to me that digital cash could be a collector's item,' remarked Hal Finney in a 1994 blog post.[14] Nick Szabo (1998b), acknowledging his own payments system, suggests that 'bit gold acts more like collectors' items than like gold.' Responding to an online forum thread called 'Bitcoins are most like shares of common stock,' Satoshi Nakamoto 'himself' emerges for one of his final public engagements,[15] replying, 'Bitcoins have no dividend or potential future dividend, therefore not like a stock. More like a collectible or commodity.'[16] Those seriously thinking about – and indeed developing – cryptocurrency rarely spoke of it in traditional monetary terms, whether from the standpoint of economics or the other social sciences, but instead as a computer-generated collectible. It is little surprise, then, that Bitcoin confounds as an object *qua* money.

Before moving on, it is worthwhile to reflect on the current value of Bitcoins, which reached as high as $19,000 in December 2017, and which trades at around $4,000 several months later at the time of writing. Whatever they are, Bitcoins *do* command value in the market, and while some degree is surely speculative, I would like to challenge assertions made that Bitcoins are fundamentally worthless. As shown, disintermediated trust can be accomplished mathematically through proof-of-work, but this requires the consumption of resources – in the case of Bitcoin, 'mining' that entails the use of electricity. While proof-of-work schemes were initially designed to disincentivize spammers, they are meant to *incentivize* the so-called miners of cryptocurrencies to protect the validity of the replicated database – to ensure that all the nodes remain honest. Few will incur the cost of proof-of-work unless they receive something of value in return. Indeed, what they receive are newly minted Bitcoins, and these must have an expected economic value consistent with the cost of securing the system (Hayes, 2017, 2018). Put differently, value appears to stem from the price paid for (the ongoing) disintermediation of trusted third parties, related to a Bitcoin's marginal cost of production (but cf. Luther, 2018).

What Blockchain Is. . .

This historical account is suggestive that the Bitcoin project was much more about technological solutions to social problems than about

reinventing money and disrupting the monetary order. And, while it may be the case that Satoshi Nakamoto intended for Bitcoin to *be* money, there is no reason to suppose that the intentions of the founders of cryptocurrencies should entirely govern their nature. What Bitcoin has done is persuasively demonstrate that property rights can in fact be securely and immutably transmitted from one actor to another without the need for conventional social structures. Whether or not owning Bitcoins is tantamount to owning money is far less important than how it is *enacted* (cf. Karlstrøm, 2014).

Therefore, let us abstract away from Bitcoin and focus not on it being money but on what it accomplishes. In doing so, I shall focus on the underlying technology, *blockchain,* which invites its socio-technological arrangement of human and non-human elements. Algorithms, encryption schemes, computer hardware, and network nodes are enlisted along with end-users, software developers, node operators, and commentators from a range of social worlds. These elements ultimately consist of two (or more) individuals brought together in a transfer of property rights – a transfer which is facilitated through an encrypted, shared ledger that is, in turn, validated and maintained by a decentralized consensus mechanism (e.g. proof-of-work). Schematically, there are three main parts of such an assemblage: (1) a direct peer-to-peer exchange between humans; (2) a shared record of the exchange (and all prior exchanges); and (3) a way to affirm the honesty of that record without consulting a trusted third party. How these elements are articulated to one another generates new ontologies.

The point of the use of the word *ontology* is to identify the various social realities constructed by particular configurations of blockchain assemblages. It is not simply that social groups come to understand blockchains differently depending on their particular worldview; rather, various ways of practicing or enacting these assemblages stage multiple versions, some of which may overlap with one another. Following Woolgar and Lezaun (2013: 323–4) on the theoretical significance of ontology in studies of science and technology, 'objects do not acquire a particular meaning in, or because of, a given context . . . Rather, objects are brought into being, they are realized in the course of a certain practical activity, and when that happens, they crystallize, provisionally, a particular reality.' Ways of thinking about Bitcoin variously as money, an asset, or a digital commodity should thus be distinguished from Bitcoin simultaneously *doing* a system of accounting or establishing particular rules of play.

Blockchain assemblages can be configured in diverse ways to achieve various goals, solve various problems, or otherwise order social action. In the following subsections I briefly sketch out three alternative configurations, or ontologies. I believe these will provoke interest among social scientists and make a compelling case for the continued study of

cryptocurrencies and blockchains dissociated from myopic notions of money: as systems of accounting; as organizational forms; and as institutions. While these proposals are not fully developed here and are intended more as a final commentary, I believe they can provide fertile ground for compelling lines of future inquiry.

Blockchains as Systems of Accounting. . .

A blockchain configured as Szabo (1998a) envisaged is capable of facilitating all sorts of direct transfers between individuals. For instance, taking the ledger to record deeds to real property, parties can transfer land without a title company and cadastre. Another ledger might instead track who owns which car, with the assemblage thus facilitating the sale of vehicles without state-controlled titling or departments of motor vehicles. One may yet record ownership of equity shares in corporations, removing the need for clerical enterprises such as stock exchanges and clearing houses. A ledger could maintain a record of voter registration and even votes themselves, providing an auditable, tamper-proof yet anonymous election count. It could document ownership of intellectual property, simplifying digital rights management and obfuscating the need for a patent office. A ledger, of course, could also record the ownership of monetary instruments.

Thus, at a certain level of abstraction, blockchains are autonomous, self-referential accounting systems. Systems of accounting are not trivial. According to Sombart (1924), double-entry bookkeeping was a social technology of calculation that laid the groundwork for the capitalist system of production itself, where capitalism and double-entry bookkeeping are absolutely intertwined. Carruthers and Espeland (1991) further attest to the importance of double-entry bookkeeping as a necessary precursor to capitalism, paying careful attention to both its technical and its rhetorical function. In particular, rhetoric around *rationality* engendered legitimacy and encouraged merchants to take up calculating assets against liabilities. Likewise, rhetorically situating blockchains as 'secured by math/encryption' allows for practical implementations of 'trustless' peer-to-peer transfers.

Some have stylized blockchains as *triple-entry bookkeeping* (e.g. Grigg, 2005), where the third entry refers either to the fact that all share a copy of the same ledger or that entries are signed by encryption and thus become immutable (Simoyama et al., 2017). Already, the concept of tokenized capital based upon distributed ledgers is a novel reality. Initial coin offerings (ICOs) are allowing early-stage entrepreneurs to raise billions of dollars in startup funds through channels not linked to traditional forms of capital like equity or debt. Moreover, these fundraising efforts have brought together venture and investor in a uniquely peer-to-peer manner, with further transfers of capital occurring on

blockchain-based secondary markets. If double-entry bookkeeping helped propel capitalism, one can only wonder what triple-entry bookkeeping might bring.

Blockchains as Organizational Forms. . .

Since blockchains exist across computer networks, layers of code can naturally be added as compact programs, or *scripts,* that direct entries into the ledger one way or another depending on the script's logic and some set of contingencies. For instance, a script may order *A pays B, X units if Y occurs*. The execution of these scripts is subject to the same level of decentralized consensus-making and security that proof-of-work provides for static transactions. Known as *smart contracts* (Luu et al., 2016), these self-executing programs can be constructed in the manner of an actual contract. There is no need for persons A and B to sign a written document, and crucially there is no need to monitor and enforce such a contract since it will execute (or not) automatically depending on whether the terms of the script are met. A smart contract can thus be anything from a wager, to a financial contract (such as a call option), to an employment agreement.

This leads to (at least) two intriguing possibilities when viewed from the lens of organization theory. The first is to consider transaction cost economics. Williamson (1979) proposed that firms exist (in opposition to matrices of pairwise contracting) because there will always exist some opportunists who will take advantage of incomplete contracts and shirk on their duties. The costs associated with monitoring and enforcing contracts are simply too great, and by subsuming production relations within an enclosed firm business can be carried out by decree instead of by contract. But smart contracts layered onto a blockchain are inevitably fully enforced and monitored by the proof-of-work mechanism at minimal cost. From this perspective, blockchains can systematically decompose firms into a pairwise matrix of peer-to-peer smart-contracts – effectively obviating the transaction-cost need for firms (see Davidson et al., 2018: 649–53).

Alternatively, Stinchcombe (1984) argues that firms are founded on a nexus of interrelated contracts that exist within and between firm boundaries. The practical application of this theory to blockchains is straightforward: bring together a succession of smart contracts that interact with one another for some singular purpose. The concept of a *Decentralized Autonomous Organization* (DAO) has been proposed, which effectively bundles together a series of interrelated smart contracts into a hierarchical structure under the guidance of some master contract to accomplish various functions such as buying and selling server time, investing in entrepreneurial activity, or even operating a driverless car (see Norta, 2015; DeFilippi and Wright, 2018). The blockchain becomes the

substrate for firm-like organizations that exist as virtual entities across the distributed network. More than conjecture, DAOs are already being created and tested in the real world. For example, Jentzsch (2016) developed one in the image of an investment fund seeking to capitalize various projects. Unfortunately, this prototype DAO collapsed after a bad actor exploited a poorly-written line of code. Despite this setback, new DAOs have been created that operate removed from the organizational structure we commonly understand as a corporation, but in essence carrying out the same sorts of tasks; that is, producing goods or services intended for the market.

Blockchains as Institutions. . .

According to Hodgson (1988), *institutions* are broadly defined as systems of established and prevalent rules that structure social interactions and expectations – that both constrain and enable certain behavior. Within this frame, North (1993: 11) asks, 'How have economies in the past developed institutions that provided the credible commitment that has enabled more complex contracting to be realized?', adding, 'the enforcement of property rights is central to credible commitment and a major historical stumbling block.' Moreover, 'formal rules are an important part of the institutional framework but only a part. To work effectively they must be complemented by . . . norms of behavior that supplement them and reduce enforcement costs' (1993: 20). North's argument here and elsewhere (e.g. North and Weingast, 1989) is twofold: first, institutions allow credible commitments that enforce property rights; and second, institutions extend beyond a rigid set of rules to include informal social devices.

As socio-technological assemblages that coordinate and enforce property rights, blockchains seem to fulfil North's definition of an institution. Moreover, because the particular instructions ('rules of play') of a blockchain-based system are prefigured, they also fit Hodgson's definition as a body that sets forth rules that shape behavior and expectations. Returning to Bitcoin, recall that the protocol is hardwired so that there will be an ultimate supply of 21 million bitcoins, to be released into circulation via the proof-of-work mechanism at a fixed rate of one block every 10 minutes, and so on. These are the rules of the game; there is no way to 'break' the rules – any attempt to do so would be futile. Bitcoin thus structures the 'policy' affecting the socio-economic system of its blockchain as well as shaping the micro-structures, norms, and interactions of the actors partaking in it. Davidson et al. (2018: 641) refer to blockchains as an *institutional technology*, 'a new way of coordinating economic activity . . . that is, actually a *new type of economic institution*.'

By radically disintermediating trusted third parties, which are themselves often paradigmatic institutions (e.g. central banks, etc.),

blockchains form credible (social) commitments through technology. But there can be a multitude of configurations, each setting out their own version of what is allowed and what is not. As an open-source project the code to create new blockchains is easy to understand, copy, and modify. Unsurprisingly, there are now thousands of blockchains that exist, copying one another's methodological framework and formatting it with their own rules and controls. Each blockchain is therefore its own institutional framework. So, when an influential faction of the Bitcoin community grew concerned that existing rules were becoming a constraint, they created their own version of Bitcoin through a 'hard fork' in 2017 (known as 'Bitcoin Cash') – setting their proof-of-work to follow a new, modified formula – where individuals can choose which institutional structure they prefer.

By creating new blockchains or breaking off from existing lines, a free market for institutions arises, with one competing against another for adherents. At the same time, blockchains are radically disintermediating institutions by maintaining the credible commitments that were conferred by them, but now in socio-technological form. However, blockchains do not merely replace institutions – they *are* the very institutions they succeed. Due to the flexible, configurable, and open nature of blockchain code, they are indeed sandboxes for institution creation and experimentation, where institutions are not only supplanted but created *eo ipso*. Novel ways of structuring social interaction through these assemblages may pave the way for new social orders, new polities, and new economies. Vitalik Buterin (2015), the co-creator of the Ethereum blockchain, puts this succinctly:[17]

> Blockchains are not about bringing to the world any one particular ruleset, they're about creating the freedom to create a new mechanism with a new ruleset extremely quickly and pushing it out. They're *Lego Mindstorms* for building economic and social institutions.

In this way, blockchains may fulfil the crypto-anarchic view of a Hobbesian *techno-leviathan* (Scott, 2015, in Dodd, 2018). Scott (2015) asks:

> Don't decentralised blockchains offer the ultimate prospect of protected property rights with clear rules, but without the political interference? This is essentially the vision of the internet techno-leviathan, a deified crypto-sovereign whose rules we can contract to. The rules being contracted to are a series of algorithms, step by step procedures for calculations which can only be overridden with great difficulty.[18]

Take as an example the blockchain EOS.[19] It is enacted with decentralized, socio-technological governance utilizing peer-to-peer terms of a

binding contract among its participants, referred to as its 'constitution' – theoretically similar in many ways to the governing documents established by nation-states. According to the EOS whitepaper:

> the content of this constitution defines obligations among the users which cannot be entirely enforced by code and facilitates dispute resolution by establishing jurisdiction and choice of law along with other mutually accepted rules. Every transaction broadcast on the network must incorporate the hash of the constitution as part of the signature and thereby explicitly binds the signer to the contract.[20]

The EOS techno-society is so ordered mutually through technological and social relations.

Blockchains as money...

Before concluding, I want to return to the notion of blockchain-based money. Even though the rules of play enacted by Bitcoin may not constitute good money, there is every reason to believe that some other blockchain governed by a different set of rules could. For instance, if money is taken to be an institution (e.g. Dillard, 1987), then a properly defined set of monetary principles and controls could be implemented accordingly. Or, if one takes money as *numeraire* – as being the ledger *itself* – in the tradition of Keynes, Minsky, and Maurer (2006), then the systems of accounting ontology could indeed be used to enact money, given that what is entered into the ledger represents a socially recognized money-thing. At the moment, several of the world's monetary authorities are embarking on projects to create central bank-backed-cryptocurrencies (CBBCs) built from blockchains (e.g. Bech and Garratt, 2017). Of course, such monies would not be decentralized; however, I argue that decentralized money is already being enacted, albeit as special cases circumscribed by the socio-technological boundaries of particular blockchains.

To illustrate this, take the native token of the Ethereum blockchain, *ether*. Ethereum is a platform built for creating and applying smart contracts, where the nodes in its network of miners act collectively as a 'virtual machine' that assesses and executes the instructions therein. Each node in the Ethereum virtual machine (EVM) evaluates in parallel the code for every smart contract and then reaches a consensus, based on proof-of-work, as to the outcome of that contract, and executes it accordingly. Processing these lines of code is computationally expensive, since every node must evaluate each smart contract in sequential order. Ether tokens are used by the system to allocate the scarce resource that is the processing power of the EVM itself. Those seeking to use a smart contract must 'pay for' the network's services by attaching some amount of ether to the contract.[21] The more computationally intensive, the more

ether must be paid. Similarly, as many smart contracts await evaluation by the EVM, more ether can be attached to a particular contract to advance its place in the queue. Thus, ether serves as the uniquely specified unit of account within the bounds of this economy as well as the medium of exchange. Ether is a machine-money, which is not human readable except when it is part of the Ethereum assemblage. As soon as ether crosses that boundary it is no longer recognized as such and must be translated (exchanged) into something else, such as euros.

Conclusion

In this essay I respond to the nascent sociology of Bitcoin by reframing it (along with all other blockchains) not as money but as socio-technological assemblages composed of a direct peer-to-peer exchange of property rights, a shared ledger of the exchange, and a mechanism to achieve consensus with reference to that ledger without resorting to a trusted third party. I first retrace the technological and ideological origins of Bitcoin starting with Chaum (1983) through to its introduction in 2009. This frames the pursuit of Bitcoin and what led up to it as a series of practical solutions to puzzles needing solving, primarily to preserve privacy and prevent 'double-spend' in a digital space, combined with the abstract social problem of relying on trusted third parties or institutions, to enforce credible commitments regarding property rights. I then propose new ontologies for what blockchains are: as systems of accounting; organizational forms of contracting in lieu of firms; and as institutions in their own right capable of ordering social behavior.

ORCID iD

Adam Hayes http://orcid.org/0000-0001-5481-8906

Notes

1. By convention, Bitcoin with a capital 'B' refers to the system, protocol, and network; bitcoin with a small 'b' refers to the individual units.
2. See: https://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
3. Who Satoshi is remains a mystery, despite attempts to reveal his/her/their identity. See Humayun and Belk (2018) for an interesting analysis of this structural anonymity.
4. Some still cite Aristotle's properties required for a 'good money': durable, portable, divisible, fungible, and scarce/intrinsically valuable.
5. See: https://sourceforge.net/p/bitcoin/mailman/message/21312004/
6. See: https://iacr.org/cryptodb/data/byyear.php
7. See: https://en.wikipedia.org/wiki/DigiCash
8. An illustration of the ring-shaped cave appears in Quisquater et al. (1989).

9. The term 'Cypherpunks' was coined by the hacktivist Judith (St. Jude) Milhon to acknowledge the spirit of the movement: the goal of privacy through encryption (where 'cypher' alludes to cipher, or coded text).
10. See: https://web.archive.org/web/20050224055704/http://www.finney.org:80/~hal/why_rem1.html
11. See: https://web.archive.org/web/19970614112136/http://www.best.com:80/~szabo/el.privacy.html
12. Szabo's blog posts, however, do show an understanding of Mengerian economic thought.
13. See: https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/hal-finney-received-the-first-bitcointransaction-heres-how-he-describes-it/
14. See: https://web.archive.org/web/20050212115346/http://www.finney.org:80/~hal/beauty_ecash.html
15. Nakamoto disappears after December 2010.
16. See: https://bitcointalk.org/index.php?topic=845.msg11403#msg11403
17. Ethereum is presently the third-largest blockchain by market value.
18. Scott (2015) isn't advocating for a world of algorithms ruling all: 'We do not want a future society free from people we have to trust... Rather, we want a world in which technology is used to dilute the power of those systems that cause us to doubt trust relationships.'
19. EOS is presently the fifth-largest blockchain by market value.
20. See: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md
21. This amount of ether is known as 'gas.'

References

Alston LJ and Mueller B (2008) Property rights and the state. In: Menard C and Shirley MM (eds) *Handbook of New Institutional Economics*. New York: Berlin: Springer-Verlag, pp. 573–590.

Bech M and Garratt R (2017) Central bank cryptocurrencies. *BIS Quarterly Review* 55. Available at: https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf (accessed 18 January 2019).

Besley T and Persson T (2009) The origins of state capacity: Property rights, taxation, and politics. *American Economic Review* 99(4): 1218–1244.

Bjerg O (2016) How is Bitcoin money? *Theory, Culture & Society* 33(1): 53–72.

Brands S (1993) Untraceable off-line cash in wallet with observers. In: Stinson DR (ed.) *Advances in Cryptology: CRYPTO '93*. Berlin: Springer-Verlag, pp. 302–318.

Broadberry S and Gupta B (2006) The early modern great divergence: Wages, prices and economic development in Europe and Asia, 1500–1800. *Economic History Review* 59(1): 2–31.

Buterin V (2015) Visions, Part I: The value of blockchain technology. Available at: https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/ (accessed 18 January 2019).

Callon M (1998) Introduction: The embeddedness of economic markets in economics. *The Sociological Review* 46(S1): 1–57.

Carruthers BG and Espeland WN (1991) Accounting for rationality: Double-entry bookkeeping and the rhetoric of economic rationality. *American Journal of Sociology* 97(1): 31–69.

Chaum D (1983) Blind signatures for untraceable payments. In: Chaum D, Rivest RL and Sherman AT (eds) *Advances in Cryptology*. Boston, MA: Springer, pp. 199–203.
Chaum D (1985) Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM* 28(10): 1030–1044.
Chaum D, Fiat A and Naor M (1988) Untraceable electronic cash. In: Goldwasser W (ed.) *Advances in Cryptology: CRYPTO '88*. New York: Springer, pp. 319–327.
Davidson S, De Filippi P and Potts J (2018) Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics* 14(4): 639–658.
Dai W (1998) b-money. Available at: http://www.weidai.com/bmoney.txt (accessed 18 January 2019).
DeFilippi P and Wright A (2018) *Blockchain and the Law: The Rule of Code*. Cambridge, MA: Harvard University Press.
Diffie W and Hellman M (1976) New directions in cryptography. *IEEE Transactions on Information Theory* 22(6): 644–654.
Dillard D (1987) Money as an institution of capitalism. *Journal of Economic Issues* 21(4): 1623–1647.
Dodd N (2014) *The Social Life of Money*. Princeton: Princeton University Press.
Dodd N (2018) The social life of Bitcoin. *Theory, Culture & Society* 35(3): 35–56.
Dwork C and Naor M (1993) Pricing via processing or combatting junk mail. In: Brickell EF (ed.) *Advances in Cryptology: CRYPTO '92*. Berlin: Springer-Verlag, pp. 139–147.
Even S, Goldreich O and Yacobi Y (1984) Electronic wallet. In: Chaum D (ed.) *Advances in Cryptology*. Boston, MA: Springer, pp. 383–386.
Golumbia D (2016) *The Politics of Bitcoin: Software as Right-Wing Extremism*. Minneapolis: University of Minnesota Press.
Graeber D (2012) *Debt: The First 5,000 Years*. New York: Penguin.
Grigg I (2005) Triple entry accounting. *Systemics Inc*. Available at: http://iang.org/papers/triple_entry.html (accessed 18 January 2019).
Hayes A (2017) Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing Bitcoin. *Telematics and Informatics* 34(7): 1308–1321.
Hayes A (2018) Bitcoin price and its marginal cost of production: Support for a fundamental value. *Applied Economics Letters*. DOI: 10.1080/13504851.2018.1488040.
Hendrickson JR, Hogan TL and Luther WJ (2016) The political economy of Bitcoin. *Economic Inquiry* 54(2): 925–939.
Hodgson GM (1988) Economics and institutions. *Journal of Economic Issues* 40(1): 1–25.
Hughes E (1993) A cypherpunk's manifesto. Available at: http://nakamotoinstitute.org/cypherpunk-manifesto/#selection-7.4-7.28 (accessed 18 January 2019).
Humayun M and Belk RW (2018) 'Satoshi is dead. Long live Satoshi': The curious case of Bitcoin's creator. In: Cross SNN, Ruvalcaba C, Venkatesh A and Belk RW (eds) *Consumer Culture Theory (Research in Consumer Behavior, Volume 19)*. Emerald Publishing Limited, pp. 19–35.
Ingham G (2013) *The Nature of Money*. Hoboken, NJ: Wiley.
Jakobsson M and Juels A (1999) Proofs of work and bread pudding protocols. In: Preneel B (ed.) *Secure Information Networks*. Boston, MA: Springer, pp. 258–272.

Jentzsch C (2016) Decentralized autonomous organization to automate governance. Available at: https://download.slock.it/public/DAO/WhitePaper.pdf (accessed 18 January 2019).
Karlstrøm H (2014) Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: Scandinavian Journal of Social Theory* 15(1): 23–36.
Kuhn TS (1962) *The Structure of Scientific Revolutions*. Chicago: University of Chicago Press.
Lamport L, Shostak R and Pease M (1982) The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems* 4(3): 382–401.
Latour B (2005) *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.
Luther WJ (2018) Is Bitcoin intrinsically worthless? *AIER Sound Money Project Working Paper No. 2018-07*.
Luu L, Chu DH, Olickel H, Saxena P and Hobor A (2016) Making smart contracts smarter. In: *Proceedings of the 2016 ACM-SIGSAC Conference*. New York: ACM, pp. 254–269.
Maurer B (2006) The anthropology of money. *Annual Review of Anthropology* 35: 15–36.
Maurer B (2017) Blockchains are a diamond's best friend. In: Bandelj N, Wherry F and Zelizer V (eds) *Money Talks: Explaining How Money Really Works*. Princeton: Princeton University Press.
Maurer B, Nelms, TC, 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 (1994) The cyphernomicon: Cypherpunks FAQ and more. Available at: http://www.kreps.org/hackers/overheads/11cyphernervs.pdf (accessed 18 January 2019).
Mishkin FS (2007) *The Economics of Money, Banking, and Financial Markets*. London: Pearson.
Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf (accessed 18 January 2019).
Narayanan A and Clark J (2017) Bitcoin's academic pedigree. *Communications of the ACM* 60(12): 36–45.
Nelms TC, Maurer B, Swartz L and Mainwaring S (2018) Social payments: Innovation, trust, Bitcoin, and the sharing economy. *Theory, Culture & Society* 35(3): 13–33.
Norta A (2015) Creation of smart-contracting collaborations for decentralized autonomous organizations. *Proceedings: 14th International Conference on Business Informatics Research*. Berlin: Springer Verlag, pp. 3–17.
North DC (1993) Institutions and credible commitment. *Journal of Institutional and Theoretical Economics*. Available at: https://econwpa.ub.uni-muenchen.de/econ-wp/eh/papers/9412/9412002.pdf (accessed 18 January 2019).
North DC and Weingast BR (1989) Constitutions and commitment: The evolution of institutions governing public choice in seventeenth-century England. *Journal of Economic History* 49(4): 803–832.
Okamoto T and Ohta K (1989) Disposable zero-knowledge authentications and their applications to untraceable electronic cash. In: Brassard G (ed.) *Advances in Cryptology – CRYPTO '89 Proceedings*. New York: Springer, pp. 481–496.

Quisquater JJ, Quisquater M, Quisquater M, Quisquater M, Guillou L, Guillou MA and Guillou S (1989) How to explain zero-knowledge protocols to your children. In: Brassard G (ed.) *Conference on the Theory and Application of Cryptology*. New York: Springer, pp. 628–631.
Rivest RL, Shamir A and Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* 21(2): 120–126.
Scott B (2015) Visions of a techno-Leviathan: The politics of the Bitcoin blockchain. Available at: https://www.e-ir.info/2014/06/01/visions-of-a-techno-leviathan-the-politics-of-the-bitcoin-blockchain/ (accessed 18 January 2019).
Selgin G (2015) Synthetic commodity money. *Journal of Financial Stability* 17: 92–99.
Simoyama FDO, Grigg I, Bueno RLP and Oliveira LCD (2017) Triple entry ledgers with blockchain for auditing. *International Journal of Auditing Technology* 3(3): 163–183.
Sombart W (1924) *Der Moderne Kapitalismus*. Munich: Duncker & Humblot.
Stinchcombe AL (1984) *Contracts as Hierarchical Documents*. Bergen: Institute of Industrial Economics.
Swartz L (2018) What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. *Cultural Studies* 32(4), 623–650.
Szabo N (1998a) Secure property titles with owner authority. Available at: https://nakamotoinstitute.org/secure-property-titles/ (accessed 18 January 2019).
Szabo N (1998b) Bit gold. Available at: http://c2.com:80/cgi/wiki?BitGold (accessed 18 January 2019).
Tasca P, Hayes A and Liu S (2018) The evolution of the bitcoin economy: Extracting and analyzing the network of payment relationships. *Journal of Risk Finance* 19(2): 94–126.
Titmuss RM (1974) *Social Policy*. New York: Pantheon Press.
Von Glahn R (1996) *Fountain of Fortune: Money and Monetary Policy in China, 1000–1700*. Berkeley: University of California Press.
Williamson OE (1979) Transaction-cost economics: The governance of contractual relations. *Journal of Law and Economics* 22(2): 233–261.
Woolgar S and Lezaun J (2013) The wrong bin bag: A turn to ontology in science and technology studies? *Social Studies of Science* 43(3): 321–340.
Wray LR (1998) *Understanding Modern Money*. Cheltenham: Edward Elgar.
Yermack D (2015) Is Bitcoin a real currency? An economic appraisal. In: Chuen DLK (ed.) *Handbook of Digital Currency*. San Diego: Academic Press, pp. 31–43.
Zimmer Z (2017) Bitcoin and Potosí silver historical perspectives on cryptocurrency. *Technology and Culture* 58(2): 307–334.

Adam Hayes is a PhD candidate in sociology at the University of Wisconsin-Madison. His research interrogates the role of financial technology in society and broadly draws on economic sociology, STS, and the social studies of finance. His current projects include social studies of cryptocurrency and blockchain, and how roboadvisors conjure rational economic man into existence. He holds an MA in economics and is a CFA charterholder.