

UC Irvine

Papers

Title

Blockchain

Permalink

<https://escholarship.org/uc/item/7m88s51d>

Author

Maurer, B

Publication Date

2021-05-27

Copyright Information

This work is made available under the terms of a Creative Commons Attribution License, available at <https://creativecommons.org/licenses/by/4.0/>

Peer reviewed

11 Blockchain

Bill Maurer

```
// Nodes collect new transactions into a block, hash them into a hash tree,  
// and scan through nonce values to make the block's hash satisfy proof-of-work  
// requirements. When they solve the proof-of-work, they broadcast the block  
// to everyone and the block is added to the block chain. The first transaction  
// in the block is a special one that creates a new coin owned by the creator  
// of the block.1
```

Archaeologists of the future trying to understand computer network technologies of the early 21st century may stumble upon something called blockchain. By that time, far from now, blockchain will have either revolutionized all computational systems and become the basis of digital identification for future persons, things, computational agents, and their various hybrids and mixtures; or it will have faded into utter obscurity, leaving barely a trace in the technoarchaeological record; or maybe it will have the status of the ARPANET today – we all sort of know it was something important that laid the foundations for the Internet, even if we don't know how, or why, or what the TCP/IP protocol is that packages, transmits, and receives electronic communications on the computer networks we use every day.

Digital media scholar Finn Brunton maps out a speculative methodology for future scholars encountering, as he did, the “digital middens” of the era of networked computing – the “accidental archives, collections of digital rubbish” (2017:139), “the accumulations of by-products and junk and trash and bits and pieces of the working life of computers and communities” (p. 141). Like the waste dumps that provide such rich material for fleshing out the contexts of life of ancient peoples, digital middens – the archival and material throwaways of networked computing – open into the hidden infrastructures and implicit value systems of those who left them behind.

For blockchain, that detritus would include textual material like the epigraph to this chapter, the notes in the source code for the original Bitcoin blockchain. It would also include the so-called cryptograffiti or messages attached by users of the system to Bitcoin transactions to memorialize an event, spread an ideology, capture an image, or simply have fun (Figures 11.1 and 11.2). There exist digital dumps, too, related to blockchain: copies of various versions of different protocols and copies of various blockchains themselves, in whole or in part, in servers,

laptops, mobile phones, and the desktop computer in one of my offices in Irvine, California. That particular computer has not been turned on since sometime in 2017, unupdated, unused, not even really strictly speaking “idle” because, as long as the machine stays off, the data constituting the blockchain on that desktop computer exists as weak electrical charges trapped in a silicon nitride film. The charges dissipate over time – so our future archaeologist would find shreds and patches, literally bits of bits, and unless equipped with some fancy future technology would likely have to hunt from among multiple desktops and servers containing the same blockchain to piece together whatever it was these humans of the past had created in those strange conductive silicon surfaces.

The materiality of computer memory raises another interesting question regarding this future archaeology of blockchain, and digital materials in general: how will our contemporary ideological separation of the digital from the material or the virtual from the physical be captured in the digital middens available to future scholars? As Paul Dourish argues, the separation of the digital from the material requires a lot of effort: digital and material are mutually embedded, and embedded in society and community (computational, human, and hybrid). “Virtual objects manifest themselves as signals, charges, and states that must be grappled with materially in digital systems and which come with their own constraints” (Dourish 2017:202), and material can afford all kinds of perceptual virtuality, presenting spectacles, dazzling the humans who mistake their physical qualities for virtues (Strathern 2013). For blockchain, the sheer magnitude of computational power it requires, and the vast server farms created to maintain it, have led to piles and piles of electronic waste, environmental hazards that at least one historian has likened to the destruction caused by colonial-era silver mining (Zimmer 2017). Adopting an anthropological stance, how will future archaeologists grasp others’ ontologies of that which I gloss as digital and material because of the sociotechnical and capitalist world within which I write (see, e.g., Bell and Kuipers 2018 for recent studies of the ontologies and intimacies of another set of digital/material technologies)?

Ten years into the history of Bitcoin and blockchain databases that sustain it and other similar “cryptocurrency” projects, it’s difficult to say how much record it will leave behind. The business and technology worlds in the US and Europe are rife with intellectual and financial speculation about blockchain, even if few understand what it is and how it works. Regulators around the globe are in the process of grappling with some of its implications. Some of the more active regulators are in places like Singapore, Estonia, Malta, and Vanuatu – an odd collection of microstates that has not a little overlap with the offshore financial services economy. As for Bitcoin, the “currency” that unleashed this interest, its value relative to the US dollar has swung wildly during the time of my writing, between December 2017 (where it stood at nearly US\$20,000/Bitcoin) and January 2019 (where it stood at just over US\$3,600). In late February, 2021, the price ran up all the way to \$57,489.

This chapter provides a chronicle from the past for that future archaeologist, situates the state of blockchain databases for the anthropologists of today, and explains some of the peculiarities of this new network technology suite. Academic

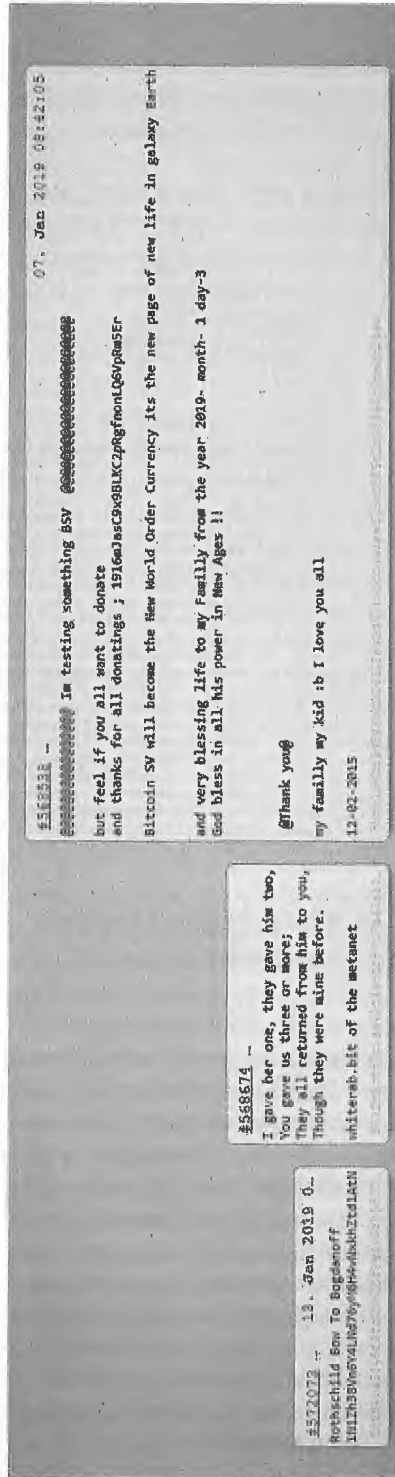


Figure 11.1 Screenshot of “cryptograffiti”: message encoded in the Bitcoin blockchain
Source: Collected by Maurer 14 January 2019.

Dr. Bill Maurer
Economic anthropologist

Figure 11.2 Cryptograffiti of the author in the Bitcoin blockchain

Source: Created by Caitlin Lustig, captured by Maurer 28 August 2017.

research on blockchain is in its infancy, yet there is a handful of anthropologists beginning to devise projects on blockchain or stumbling upon it in their existing fieldsites. Most of the work on the phenomenon that is not computer science is coming from communications scholars. This chapter is not a literature review, however, but a primer on blockchain for digital anthropology with some suggestions for method. Blockchain and cryptocurrencies provide new material for economic anthropology's enduring questions about the relation between money, politics, and commodity fetishism. Anthropologists can also use blockchain to query globalization in its digital forms, the creation of new localisms through globally networked digital media, or the contests over digital commons and their enclosure. Taken as media, blockchain raises questions about reproducibility, mimesis, and how digital media write their own historiographies. Whatever its futures, blockchain is good to think with.

Ultimately, I view blockchain as an interesting note in the history of accounting, more so than in the history of money, though it signals the revivification of some very Austrian economic theories on the nature and authorization of money, as I discuss in what follows. As an accounting technology, blockchain is being inserted into conversations in the technology and the business world about automation and “disintermediation.” The former is founded on the idea that blockchain can begin to automate various kinds of decision-making and action in the physical world and/or in the world of communication among connected computational devices – a future of work without human labor. Think of a digital system for tracking the provenance of goods in a supply chain, whether digital or physical goods. The latter, disintermediation, is a keyword in blockchain communities that indexes both an anti-state or outright anarchist orientation toward liberal political institutions, an anti-bank or anti-central-bank commitment to “direct” economic relationships among transacting parties, and/or a related desire for unmediated, “peer to peer” communications channels (including money as a communicative practice; see Swartz 2018). These are political positions, and they stake out territory on the libertarian right and, perhaps to a lesser extent, the cooperativist left.

Blockchain has opened up a public conversation over the politics of infrastructure. And at stake is the control over the infrastructures subtending economic-communicative relations. Insofar as blockchain helps illuminate these political positions, it is a useful case study for the potential transformation of neoliberal economies and political institutions that has been going on since the global financial crisis of 2008.

Money in the age of digital reproduction

For our future technoarchaeologist, there will likely be archival traces of something called the Satoshi whitepaper, and this is as good a place as any to begin. “Bitcoin: A Peer-to-Peer Electronic Cash System” (Nakamoto 2008) was written under a pseudonym of a programmer or a group of programmers. The paper proposed a digital cash system that would solve some of the problems inherent to creating digital objects of value. It also inaugurated a genre: the cryptocurrency “whitepaper.” Whitepapers accompany almost all blockchain projects. In keeping with the Bitcoin blockchain’s open source ethos, they are generally publicly accessible and sometimes even contain source code for the projects they promote. Posting a whitepaper is akin to announcing one’s existence and is almost a prerequisite for entering into the blockchain developer community. During the huge run-up in the prices of cryptocurrencies in 2017, whitepapers also came under regulatory scrutiny because they have the function of advertising a project in order to solicit investors. Depending on the kind of project and the kind of fundraising suggested in the whitepaper or by the proposed technology itself, a whitepaper can be taken as a solicitation for investment in an unregistered security.

Chief among the problems Nakamoto sought to solve was the “double-spend” problem. In a digital environment, duplication of any data is relatively easy

and often cost-free, both economically and computationally. Just as I can copy and paste an instance of a word in the electronic document I am composing as I write this chapter, so too a digital “thing” of value can usually be duplicated and reduplicated.

The first section of Walter Benjamin’s (1936) classic *The Work of Art in the Age of Mechanical Reproduction* chronicles the history of the copy, of reproducibility by technical means. In photography, the use of the negative to make multiple prints obviates the whole notion of their being an “authentic” print. This transforms the nature of art, he argued. In confounding the notion of originality, photography liberated art from the burden of authenticity. According to Benjamin, this in turn took art from the domain of ritual and into that of politics: with the loss of the work’s supposed connection to the specific contexts of the timespace of its creation, a mechanically reproduced version of the work could be enlisted into the service of political praxis. Anthropologists of art and cultural property are familiar with the political and cultural conundrums raised by the separation of a work from its lived social contexts, its reproduction for new uses and markets, and even its demarcation as “art” or “culture” – which can in turn make it subject of new political and property relations (Errington 1998; Price 2002; Myers 2002; Geismar 2013).

It is apt that in the beginning of Benjamin’s essay, money makes a brief appearance – not explicitly due to its mechanical reproducibility as a form of politics but as one of the earliest instances of technological reproduction. Benjamin began his essay with what he considered to be the only form of “technically reproducing works of art” among the ancient Greeks – “founding and stamping” – and says that each of the Greeks’ creative productions were unique, except for those made by these two techniques. Those included pottery, bronzes, and coins. A political invention par excellence, the coin was instrumental in elites’ extension of sovereignty (Shell 1978). It nicely proves Benjamin’s point about art and politics.

Eliminating the “double-spend” problem, as Satoshi’s proposal sought to do, was a move to disallow copying and thereby evacuate politics from the work of money creation. Satoshi and those who followed were not just worried about copying in the form of counterfeiting. The politics they had in mind was specifically that of states’ and banks’ role in making money, creating it seemingly ex nihilo. Anthropologists have long documented people’s puzzlement in encountering modern, Western, capitalist money, precisely because the source of its value is so opaque and because they sought to play other kinds of games with it than strictly economic transactions (Strathern 1975; Foster 1999). Satoshi and his peers sought a means of bringing into the world a singular, unique value, a money each unit of which was itself distinct and unique – right down to the very code on which it is built, as I describe later. To be more specific, Satoshi and Satoshi’s followers believed they were creating a money that would be sustained by a network of peers rather than any state, government, or other kind of intermediary institution like a bank. It would be done by “just us,” a vision not of a community so much as a distributed collection of individualized nodes – human or otherwise (Future of Money Research Collaborative 2018). The idea that money is not political,

of course, is also part of its ideological trappings – the state sets the standard, as anthropologists and historians of money continually point out (Gregory 1996), or, if not the state as such, then political authorities invested in sustaining systems that maintain their own high status (Maurer 2018).

Despite utopian proclamations of being the next step in the evolution of money, the harbinger of decentralized, disintermediated value systems maintained by networks of “peers” without the need for law or other institutions (which proponents gloss as “trusted third parties” or “trusted intermediaries”), blockchain adherents, themselves ideologically diverse, view “trustless” systems maintained by “the code” as a good in themselves. Their deep suspicion of the state and of traditional financial intermediaries like banks belies how many blockchain companies seek to position themselves as new intermediaries. It also glosses over the extent to which, so far in their history, cryptocurrencies are mostly not functioning as money but as speculative assets (although some people in countries with currency restrictions or highly unstable state-issued money are finding uses for cryptocurrencies beyond hoarding and exchanging them). Although some online and physical world vendors accept cryptocurrencies as a form of payment, the currencies’ price volatility makes using them as such an irrational choice. Instead, most activity takes place on virtual exchanges, where they are traded for one another and for what blockchain adherents call “fiat,” that is, state-issued currency (which is created, again, *ex nihilo* – fiat lux! – my Latin references being intentional, as it is the ascription to the state and banks of the god-like power to create that enervates and motivates many cryptocurrency proponents).

Uniqueness or singularity. Trust and trustlessness. Decentralization and disintermediation. These are the keywords of blockchain. It is important to remember, however, that reproducibility was the central problem Nakamoto sought to solve.

Digital chains of custody

By the end of the 20th century, the owners of digital intellectual property had adopted numerous legal and technological strategies to deal with the reproducibility problem, classed under the umbrella term digital rights management (DRM). DRM strategies included hardware- and software-based methods to prevent copying. One of the oldest involved requiring users to enter a secret code or a serial number printed in a paper book or on the paper, cardboard, or plastic packaging of physical storage media containing a digital product in order to use that product. For money, however, the problem is compounded by the fact that to function as a medium of exchange, a digital money must pass from user to user – if not from physical hand to hand – or at least be represented as having changed ownership multiple times throughout its existence, potentially into infinity. It has to be able to do this – at least given our contemporary monetary imaginations – without each individual token multiplying itself or being multiplied. For it to function as money (again, given our current limited imagination), it cannot be reduplicated or redenominated by anything other than the authority that produced it – in our case, the state.

Given this system requirement for circulation without unauthorized reduplication, Nakamoto sought to develop a procedure that would prevent malicious users from taking one instance of digital value, duplicating it, and using it more than once, that is to prevent users from creating new digital value from a set pool of it. Given the commitment to eliminating third-party intermediaries, Nakamoto sought a networked solution to the reduplication problem. And given a commitment to anonymity in transactions mirroring cash – a commitment reflected in Nakamoto's own anonymity – Nakamoto sought a digital identity system. The solution therefore involved four main parts:

- A peer-to-peer network, so as to avoid the need for a third-party validator or verifier of transactions
- A method for timestamping transactions
- A method for ensuring the ownership claims of transacting parties
- A method for ensuring the digital identity of the transacting parties without revealing those identities

Nakamoto did not refer to a “blockchain” in the paper. But the notes to the original source code, reproduced in the epigraph to this chapter, explain that a “block” of transactions is added, after some additional computational work, to a “block chain.” The whitepaper refers to an “ongoing chain” of transactions (p. 1) and once (p. 7) to a “chain of blocks.” Within a year or two of Bitcoin's creation, the database underpinning the Bitcoin cryptocurrency came to be known as “the blockchain” or simply “blockchain.”

Blockchain refers to a database with some distinctive features. First and foremost, multiple copies of it exist and are held by multiple parties in a network. Generally, people involved in cryptocurrency and blockchain-related businesses refer to this feature as being “distributed.” A truly distributed database, however, would be disaggregated into constituent components, each component held by a node in a network, such that the whole could only be knowable through the participation or agreement of the entire network. The whole would consist of pieces distributed among multiple parties. Blockchain does not work this way. Instead, the entire database in multiple instances is held by the nodes in the network. Each node has a copy of the whole thing in order to ensure that changes to the database cannot take place without having gone through a specific verification procedure involving all the nodes. If one node makes an unauthorized change to prior entries in its copy of the database and then shares data with the network or just another node, the other nodes should be able to spot the change. The protocol involved refuses such transactions.

Second, blockchain databases are “append-only.” This means that old entries are never revised. Any change to an old entry must be made by following a protocol that adds a new entry to the database. The database is continuously expanding as a result. Bitcoin's inventors, however, gave it a fixed limit of 21 million Bitcoins. They did this for monetarist ideological reasons deriving from Austrian school economics, holding that any intervention in market relationships would

interfere with the freedom of individuals to transact. Money should be a scarce commodity subject to the same laws of supply and demand as other commodities. Rather than a government increasing the money supply, however, and thus interfering with the value of money, F.A. Hayek (1976) went so far as to propose the denationalization of money altogether and the creation of a competitive market of multiple private currencies.

Bitcoin's inventors also limited the amount of Bitcoin to solve a technical problem: fixing the amount of Bitcoin ever to exist helped support the verification procedure the network undertakes. The blockchain is potentially infinite and ever expanding. Its append-only nature means it will get bigger and bigger and bigger, until the computational networks maintaining it can no longer sustain it. Placing a "hard cap" on the number of Bitcoin ever to be mined mitigates the problem of database expansion.

It also lends itself to another feature: every entry is time-stamped, and time progresses linearly in a blockchain. It is a serialized, ongoing record of transactions. And, again, old transactions cannot be modified; changes involving old transactions – which is what any transaction in the blockchain actually is – become new entries appended onto the database. That it unfolds in real time, constantly moving forward in time, makes it resemble a digital chronicle more than a digital history: there is no hierarchization, or the elevation of one entry or set of entries over the others (see Brunton 2017). It is one damn thing after another. Individual Bitcoin transactions can be speeded up, however, and made to settle faster than others, as the nodes that serve as transaction verifiers ("miners") can assess fees to facilitate transactions by in effect moving them up in the queue.

The Bitcoin blockchain is also public: even non-participants in the network can view the transactions in the blockchain, in real time. Depending on what application they use to view the transactions, what they will see is something like this:

2018-12-01 16:37:20

3QwcnREdSxefKhweCiRwzczwU7f9zSaDV4k

1LA1f3X7rpEVkSLEezq6Kbt13cdQF6zLQ 0.00936694 BTC

3BcVWDcjwTjGgVNJsWowyaLDe7ANbTBmQC 0.01000005 BTC

2018-11-27 04:44:22

3QwcnREdSxefKhweCiRwzczwU7f9zSaDV4k

1GWugYqDG5voThwG8YeRPvmbyZeghTCcq1 0.00768251 BTC

31iUswoeqPTF4VAKJYvLkQ9MJVJ6it1nMh 0.0098855 BTC

You can see that the data is time-stamped. Each transaction is identified as a transfer of value from one digital address to another. In this case, the address 3QwcnREdSxefKhweCiRwzczwU7f9zSaDV4k has engaged in two sets of paired transactions. (The underlying code calls for this duality in transactions, for reasons having to do with preserving the singularity of transactional records, and the digital metallist ideology of its developers [Maurer, Nelms, and Swartz 2013],

that is, their resemblance to historical goldbugs not just because of their monetary theory but also because of something they baked into the code which requires this transactional duality, to be explained later).

The Bitcoin blockchain maintains pseudoanonymity by using a digital addressing system to identify transactional partners. This system is derived from public key cryptography, a technique that allows a public address to be generated by a random number (called a private key). The private key serves like a secret password to verify the identity of the transactor but cannot be back-calculated from the public key (see DuPont 2018:60; for a history, see Blanchette 2012). In the earlier example, the digital addresses are generated by the public key – the private key is held by the entity associated with the public address 3QwcnREdSxefKhweCiRwzcwU7f9zSaDV4k.

New entries to the database are validated by a process through which individual nodes compete to verify the integrity of the transaction – that there has been no double-spend anywhere throughout the chain of transactions leading to the current one. This is done through a computational puzzle that both provides the incentive to compete for a reward denominated in Bitcoin and creates a throttle on the creation of new Bitcoin. The difficulty of the puzzle is set by the protocol to increase over time. This has led to centralization in “mining,” with conglomerates of “miners” (called “mining pools”) engaged in a hardware arms race so that they can devote more and more computational power to solving those puzzles. In this respect, Bitcoin mining resembles historical examples of actual mining in which artisanal extraction and smelting gave way to more chemical- and capital-intensive processes (Zimmer 2017).

When a new transaction is accepted as valid, it is then posted to the entire network in order to update every copy of the database on every node. This takes place only after two conditions are met: an individual node has won the competition to validate a transaction, and the consensus of the nodes agrees that its solution to the competition is valid. This in turn entails validating the transaction: solving the puzzle set forward in the competition involves using the data from the transaction in question; if it is not valid, the solution to the puzzle will not be valid, either. This process obviates the need for a central server operating as an accounts keeper.

One challenge of describing blockchain and cryptocurrencies is that the metaphors are, as one proponent and explainer puts it, “broken”:

In Bitcoin, every single term and design metaphor is absolutely and 100 percent wrong and broken. . . . A wallet is something that stores money – not in bitcoin it isn’t. The money isn’t in the wallet. The money is on the network. The wallet contains keys. So, it’s not a wallet, it’s a keychain. . . . Bitcoin. Coin – what a terrible, terrible word. What a terrible brand. Coin – take the most abstract form of money we’ve ever created that is based on a completely decentralized network that has no coins and then name it Bitcoin. Just to confuse everyone.

(Antonopolous, quoted in Torpey 2015)

Blockchain is thus a database with a complicated updating procedure, managed by a network of participating computers, each of which holds a copy of the database in toto. Because it gained prominence with an experiment in digital money, its discursive context is full of metaphors that befuddle it. As Antonopolous exasperatedly remarks, there are no “coins” or representations of digital objects of money in the system. Instead, there are messages indicating transactions in specific amounts of “Bitcoin,” marked with digital signatures derived from the cryptographic transformation of a key/message pair. Each new transaction depends on a prior transaction, not the identity of a prior transacting party. In fact, unlike 3QwcnREdSxefKhweCiRwzcwU7f9zSaDV4k, I do not need to use the same public/private key combination each time I want to transact. The system does not require it. I can create a new key pair for each transaction (and, indeed, if I am really interested in maintaining anonymity, this is what I should do, otherwise a clever computational agent could deduce my identity based on the reused public key’s prior transactions). But people tend to reuse the same key pair because they think of it as a username.

As a networked communicative infrastructure in which digital chains of custody are established among key/message units, themselves bundled together and encrypted as a unit that forms the basis of the next entry in the database, blockchain can be metaphorized as a distributed ledger – as I (Maurer 2017) and many in the blockchain community have done, particularly as the technology gained some legitimacy and investors shied away from words like “cryptocurrency” or even “blockchain” itself – but even this, as Antonopolous would say, is a broken metaphor. Again, as noted earlier, a distributed ledger would be a ledger that is divided up into pieces, the pieces distributed among a network of computers, with the whole knowable only through the participation of each node in the network sharing with the others its own, unique piece. In the case of the Bitcoin blockchain, however, every full node in the network has the complete ledger. It is more of a massively replicated ledger than a distributed one.

Market models in the code

The transaction verification system called “mining” provides a window into the politics of code. Most blockchain systems rely on what is called a proof-of-work system in order for miners to have the privilege to verify a transaction. To verify a transaction, a node takes the proposed transaction (actually a hash or digital fingerprint of the proposed transaction) and is provided an output of a complex computational operation. The node has to “guess” the inputs to this operation that will generate that output. One of the inputs is the hash of the transaction itself. The other is referred to as a “nonce” from a term for anything that has only one purpose. (Think Chaucer: “A cook they hadde with hem for the nones/To boille the chiknes with the marybones” [A cook they had with them for the sole purpose of boiling the chickens with the marrow bones]). Miners go through a process of guessing the nonce to generate the predetermined, correct output. They could

verify the transaction without this step. Proof-of-work makes the process more difficult and raises the stakes in incentivizing transaction verification: the faster I can run through potential solutions to the nonce, using more and more computational power, the greater my chances of finding it. Miners who find the nonce – and post the hashed transaction to the blockchain, where it is then verified by all the other miners (who can just take the correct nonce and plug it in to see that indeed it generates the correct output) – are rewarded in new Bitcoin. The system was set up to increase in difficulty as the maximum 21 million Bitcoin limit is reached.

The process consumes great quantities of computational cycles and electricity. By 2017 it had become common in blockchain circles to worry about all that electricity, and in that year it was reported (Digiconomist 2017) that the Bitcoin blockchain ranked between Denmark and Ireland in terms of total energy consumption. But why go to all the trouble? The answer lies more in ideological commitments than technology.

In 1993, Cynthia Dwork and Moni Naor proposed a proof-of-work system to solve a problem besetting early electronic mail. Email was “free” of cost to the sender – there was no monetary price attached to sending an individual email, even if Internet service providers charged for access to the network. In the early days of email, advertisers and other bulk users of email could exploit its lack of a monetary price and send thousands or even millions of messages. Spam was born. Dwork and Naor proposed an ingenious solution to the spam problem: attach a price to every email and require receiving servers to verify that that price had been paid. The price was not monetary, but computational. They devised a system that demanded a tiny bit of extra computational work to be conducted in order to send each email. For the individual user sending messages on the order of scores or hundreds, this extra computational effort would go unnoticed – in terms of computational speed or central processing unit cycles devoted to the task or in terms of electricity consumption (or its byproduct, heat generation). To a spammer, however, proof-of-work would impose a real cost in computational time, electricity, and heat, rendering it less profitable.

Dwork and Naor treated email like a commons pool resource, and wrote in code a strategy for dealing with it in much the same way that economist Garrett Hardin (1968) proposed a solution to the so-called tragedy of the commons. Arguing that free access to commons pool resources will inevitably lead to their degradation and depletion since each self-interested economically rational agent will try to take for itself as much as it can get, Hardin proposed putting a price on and creating markets in common goods. Left unexamined was the possibility of public, cooperative, or collective ownership or management of such resources, arrangements anthropologists have documented (see Agarwal 2003 for a review).

Other market models inform blockchain systems. The consensus model is essentially a derivative of earlier explicitly market-based systems for allocating computational resources. Mark Miller and Eric Drexler, two computer scientists who cite the impact of Austrian school economics on their thinking, devised what they called “agoric systems” for computational resource management, a

market-derived allocation or bidding system (Miller and Drexler 1988). Vitalik Buterin, founder of Ethereum, and others in the blockchain community adopted the language of agoric systems for their own projects, especially voting or blockchain-based governance-without-government projects.

That libertarian market models inform blockchain systems should not be that much of a surprise, given their origins in communities of coders whom Swartz loosely groups under the term crypto-anarchy. Most blockchain systems have relied on achieving consensus on transactional validity through monetarily incentivized competition. Or, “monetarily,” since the “money” here is not state-issued currency but chains of custody in digital message/signature combinations that are imagined as monetary tokens.

But there’s more. Because of the way blockchain solves the double-spend problem, every transaction has to be treated as unique and singular (see Dallyn 2017, following Karpik 2010 on economic singularities). And now we come to how Bitcoin’s digital metallism, its adherence to a theory of money aligned with the gold standard, is in the details of the code itself. As we saw previously with our friend 3QwcnREdSxefKhweCiRwzcwU7f9zSaDV4k, most Bitcoin transactions are dual. What is happening is that the algorithm searches for an unused message/signature of a certain denomination or value in Bitcoin (and unspent transaction output, or UTXO – the output from a prior unique transaction that has not yet been attached to a new message indicating a new transaction). It then initiates two transactions: one in the amount of the intended transfer, and the other in the amount of the “change” from this transaction, which is then “paid back” to the address initiating the transaction. This operation sutures the metaphorical relationship between Bitcoin or any cryptocurrency modeled on it to a physical world commodity. It makes it make sense to say that every “piece” of Bitcoin is itself unique. It is as if one party has a digital rock that has to be broken into two pieces in order for the one piece of the intended value to be transferred to another party. The other piece, the remainder, is transferred back to the first party. So even if a user goes beyond the metaphors Antonopolous decried and digs into the code itself, one finds operations that lend themselves to the identification of messages/signatures with a physical hunk of gold.

It is also ironic that such messages/signatures can be thought of in money terms probably only because of the existence of exchanges – the new intermediaries of the blockchain world. These exchanges allow users to purchase rights to those chains of messages/signatures, using state-issued money. Participants envision such transactions as taking a token “out” of the blockchain system – when what has really been taken out, or taken anywhere, is state-issued money from one user’s bank account to another.

Other models than proof-of-work operate in blockchain systems, some to mitigate the energy problem, others to recentralize blockchains among a narrower set of “peers.” So-called permissioned systems are often closed to outside parties and work according to a buy-in or “proof-of-stake” model. But lest the economic singularity of a Bitcoin transaction be seen as far outside the mainstream, contemporary EMV (Eurostar/Mastercard/Visa) transactions – using a chip embedded in a

plastic card to authorize credit and debit card transactions – also generate a unique identifier for each and every transaction (see Maurer, 2020). Digital records of such transactions will likely also puzzle our future archaeologist.

Anarchists and mutualists

Nakamoto's solution to the double-spend problem was thick with a specific ideology of money and of governance. That Nakamoto wanted to obviate the need for a third-party intermediary and instead establish a peer-to-peer system speaks to longstanding and specifically American criticism of banking institutions and central banks in particular. Much has been made of the link between Bitcoin and right-wing libertarian political thinking (Golumbia 2016; Brunton 2019), as well as the message hidden in the so-called genesis block – the first block of Bitcoin transactions – which has been interpreted as a criticism of banking institutions in light of their role in the 2008 global financial crisis (GFC): “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks,” referencing the headline of the Financial Times for 3 January 2009. For Nakamoto's part, the original whitepaper discusses money in relation to a “mint” (Nakamoto 2008:2), that is, a government entity which produces the money, not a bank which serves as an intermediary among transactors. Golumbia traces Bitcoin's right-wing ideology to anti-Federal Reserve conspiracy theories from the 1950s (Golumbia 2016:19), but ever since its founding in 1913 the United States' central bank has been seen as an example of federal overreach if not downright tyranny (Medley 2014:54–56). Tyranny and liberty are twinned in the lexicon of right-wing extremism in the United States (Golumbia 2016:11). Nakamoto's early readers embedded a conversation over “liberty” into a plan for a new money.

There are least two overlapping social sources for this concern with money and liberty. As Lana Swartz (2018) explains, one is the community of “cypherpunks” advocating privacy in digital networks. Realizing the potential for digital communications networks to create a new panopticon for corporations and governments to peer into anyone's digital identity, contacts, movements, and activities, cypherpunks sought to give humans the ability to control access to their digital data trails. Their focus was on building “shared communication systems that would form the basis of a new society predicated on privacy” (Swartz 2018:626).

The other is the community of “crypto-anarchists” advocating freedom from state constraints in all affairs. Technologically inspired libertarians saw in noncentralized digital networks like the Internet the possibility of freedom from any state control over anything, from communication to individual decision-making to economic exchange. In order to hold onto this dream, of course, they had to deny the role of the state in helping create and maintain infrastructures, to say nothing of the electricity grid and other systems necessary to facilitate digital networks.

Swartz further identifies two approaches to cryptocurrencies and blockchains emanating from these two overlapping social groups. The first emphasizes the work of building privacy-focused (digital) institutions and infrastructures and the collaborative, collective maintenance of such institutions and infrastructures.

The second emphasizes an imagination of money as existing outside and beyond the state and its infrastructures, given by the nature of the cryptographic protocols involved in systems like Bitcoin and subject to “natural” constraints explicitly modeled on gold. The former she terms infrastructural mutualism. The latter, as I’ve been using it in this chapter, is digital metallism (see also Maurer, Nelms, and Swartz 2013).

Swartz’s analysis is instructive for illuminating the loosely organized social movements behind blockchain, given that there remain few social scientific studies of its actual user base (but, for an early attempt, see Lustig and Nardi 2015). It also helps separate out how blockchain has unfolded between 2008 and 2018, as the tendencies toward emphasizing the collaborative coordination and upkeep of digital distributed databases on the one hand and the making of digital cash on the other have vied for prominence. In 2014, Swartz, Nelms, and I were pretty confident that the former would win out. The networks of people involved in cryptocurrencies and blockchain work seemed to be professionalizing; new companies were forming and existing companies including the major investment banks (Maurer 2016) and payment providers (like Visa and MasterCard, among others) had begun looking at blockchain to trim financial clearance and settlement times, solve complex coordination and collateralization problems in securities trading, or speed crossborder money transfers. While not necessarily “mutualist,” these were surely infrastructure builders, thinking about blockchain as the next wave of digital infrastructure for record-keeping and facilitating transactions of all kinds. Ethereum, a blockchain system released in 2015 and focused on these sorts of infrastructure and coordination problems, seemed to represent a step in the same direction.

Yet Ethereum, like most blockchain systems up to 2018, relied on a similar incentive structure for participating nodes in the network to validate transactions. And that incentive – in the case of Ethereum and most other blockchain systems – was metaphorically represented as a valuable token or currency-like unit. This sets up the system as more money-like than mutualist. That different blockchains’ tokens are convertible into one another and into state-issued currencies only made the association between them and “money” even tighter. Announcements of major investments by established and recognizable global companies like IBM, Intel, JP Morgan, and Walmart lent legitimacy to the endeavor; more people – now “investors” – literally bought in, not by participating in the work of maintaining the database by becoming a node but simply by buying the digital units associated with a blockchain on an exchange.

In 2017, the prices of all extant cryptocurrencies skyrocketed. Startups got into the act, and many people with a programming background, in the payments industry, and in banking and financial services and other sectors realized they had better chances of raising funds for a new venture by floating a blockchain project than seeking venture capital from traditional Silicon Valley or Wall Street firms. They solicited investors who would purchase (sometimes pre-purchase) the digital tokens that form the basis for reward in their blockchain’s proof-of-work system. This was the birth of the International Coin Offering (ICO) phenomenon,

modeled on startups' initial public offerings – and soon the target of regulators concerned that ICOs resembled nothing so much as unregistered sales of unauthorized securities. Regardless, an ICO bubble ensued with projects ranging from the plausible – systems using blockchain to track the provenance of baby food to ensure it is not counterfeit – to ridiculous – “DentaCoin,” for people to win a cryptocurrency for posting reviews of dentists, or celebrity-branded “coins” with no discernable purpose like CentraCoin, backed by music personality DJ Khaled and the boxer Floyd Mayweather Jr. and which ran afoul of securities regulators.

The bubble began to burst in late 2018. Journalists began to sound the death knell. Yet this had happened before, when the first Bitcoin bubble saw the currency trading at US\$1,000 in November 2013, before falling again to around \$200 throughout the next 18 months. It seems premature to write off the phenomenon just yet. And indeed, in early 2021, in the midst of the coronavirus pandemic, its price skyrocketed.

Swartz argues that Bitcoin will remain interesting for social science and critical inquiry because it crystallized early 21st-century technoeconomic imaginaries. It is also a convening technology, bringing together diverse constituencies that otherwise might never have met, such as experimental artists, money utopians, and investment bankers – literally in the same physical space (Baym, Swartz, and Alarcon 2019). The post-2008 financial crisis world opened up established verities for political contestation. From banks to governments to the tenets of liberalism and the global capitalist economic order themselves, institutions that had been relatively secure in their position and authority since the end of World War II have been questioned by increasingly vocal and powerful populist and anti-state movements and agents. Again, digital networks seem to lend themselves to unleashing reformation or outright dismantling of these institutions, and many diverse constituencies want to get in on the act, not least because the stock market went “sideways,” as an informant put it to me, after the financial crisis. Renewed skepticism of banks and regulatory agencies alike put wind in the sails of libertarians. Digital networks seemingly allow direct, unmediated communication, “peer” connection without the intercession of gatekeepers, filters, or agents to authorize this or that perspective or organization. In reality, of course, digital networks themselves are newly empowered intermediaries whose power derives precisely because it is masked by the ideology of pure “peer” connection, or of being exactly and without remainder or externality “the social network” entire.

Blockchain is interesting in this context because even though it may have inspired a frenzy of intellectual and financial speculation, and even though it is tethered to these ideologies of disintermediation and populism, it is not a free-for-all. Quite the contrary. Blockchain purports to provide a means for a distributed, decentralized network of computational agents to create and maintain a “permanent, verifiable, unalterable version of truth.” I put these words in quotation marks because they are so frequently intoned but – appropriately, perhaps – I do not believe there is one authoritative source to which it could be attributed. The phrase is so commonplace as to serve as a creed or incantation, calling forth, *abracadabra*, the truth it names.

Blockchain anthropology

I have tried to hint at why this should be interesting for anthropology along the way. Blockchain tugs at several longstanding concerns of the field, from the nature and politics of money, to the creation and negotiation of the commons, to the culture of the copy and the problem of authenticity.

Digging into the blockchain helps illuminate how people think about the digital and money together and the shifting cultural politics of the institutions and infrastructures of money. My colleagues and I have argued that things like blockchain and associated payments industry attempts to disintermediate established payment providers and the banks are opening up for discussion both the nature of money and the nature of the social. After all, what is a society of “peers,” or of “just us” (Future of Money Research Collaborative 2018)? Current challenges to liberal world orders seem to bear out the contemporary viability of anarcho-nihilist political positions and the idea of a future non-society of atomistic individuals whose associations are purely transactional.

Anthropologists have also started happening upon people around the world actually using blockchain and cryptocurrencies, sometimes with surprising reversals of the ideological positions on which they are founded. Most of this work is not yet published. For example, late in 2017, Peter Graif reports, the Nepali authorities arrested several Bitcoin miners and the owners of BitSewa, the country’s most prominent cryptocurrency exchange. People in general held negative views of miners since they were seen as enriching themselves using publicly subsidized electricity. But unlike the US, where cryptocurrencies are not really used to buy things, in Nepal people purchased digital goods online from the US, Singapore, and Europe with them. Cryptocurrency enthusiasts had formed small, rather intimate social groups, meeting at coffee shops in order to get around the country’s foreign exchange controls. A system designed to be purely digital and anonymous instead fostered a new kind of in-person community. In this context, however, exchangers like BitSewa faced another criticism than just their use of electricity: as they sought out new exchange partners outside those social circles, they were seen as breaking the trust of these nascent communities. Graif reports that one of his interlocutors said, horrified, “They were selling bitcoin to people they don’t even know.” In Nepal, he writes, Bitcoin forms new social ties while permitting “access to anonymous markets outside Nepal” (Graif, personal communication, December 2018).

Taylor Nelms (2015), working in Ecuador, writes of the “monetary mixup” that took place when the Ecuadorean and global press mistook an Ecuadorean state mobile money project for both a blockchain-based project and a state ban on Bitcoin. It was neither. Nelms shows, however, how the debate tapped into long-simmering questions about the endurance of value after Ecuador’s dollarization. Gretchen Bakke found that small-scale energy producers imagine blockchain-based systems for “transactive energy” to facilitate a new, distributed, and decentralized grid (personal communication, November 2018). Elizabeth Ferry,

working on gold, asks how gold's capacity to be a sign is based on its claim not to be a sign at all (2016:77) and that claims about Bitcoin as existing only in the code or being governed in a non-governing, trustless system, replicate that claim.

In allied fields adjacent to anthropology, scholars are considering utopian blockchain dreams in cooperative movements – and what happens in practice (Feria 2019), as well as blockchain's potential for fostering a kind of economic plurality. Plurality, however, might also encompass forms like slavery – and in my own research I have repeatedly come upon explicit and implicit invocations of a future world of enslaved computational agents managed by distributed ledger systems.

These examples show that although blockchain has primarily been located not so much in globally distributed computer networks as in the contemporary metropolitan centers of computational power – the US, Europe, and increasingly China – it has been taken up for various projects around the world. Its meanings and practices are reconfigured in the process, and some of its precepts, like anonymity, are reset, much as anthropologists have found for other money and accounting technologies.

This brings me back to my initial claim about blockchain as an accounting technology and toward a query for my imagined future archaeologist. Renaissance double-entry bookkeeping provided a vision of truth. It derived from a specific moral order (the subject as orator of his moral progress, as discussed by Aho 2006), instituted a new way of understanding “facts” (as discussed by Poovey 1998), and centrally animated the economic relations of capitalism. These relations found their fullest form – relying crucially on double entry – in the transatlantic slave trade (see Baucom 2005).

Blockchain also provides a vision of truth and derives from a specific moral order, arising in technolibertarian or anarcho-libertarian philosophies and deriving from very specific notions of the economy as agoric (which is, after all, an evocation of ancient Greek systems of political domination and enslavement, see Maurer 2020). They create a new regime of facticity, allowing for the imagination of everything as a singular, discrete unit of information that can be permanently, unalterably recorded on a distributed ledger that everyone can see and that can exist on every computational device of sufficient power.

This is not the panopticon, however. Rather than one central seeing point or place of perspective, the evidence of the fact can be “everywhere,” available to all, and eternal, in a massively replicated database held by potentially “everyone” – or at least every computer with enough storage to hold it. But it is not radically democratic. The political morality is complicated. It obviates the relations of control that older systems instituted. What does it institute in their place? In supply chains or electricity management, for example, blockchain can permit multiple, radically different systems to exist on the “input” side without the need for standardization. So long as relevant data can be entered into a distributed ledger, existence can be recorded and thereafter forever tracked as verified and true. How something came to be is immaterial, if the mere fact of being is what is at stake. Blockchain can thus provide a platform for plural and alternative economies to interoperate. This

means, in theory, we can have both communal, regenerative agriculture and plantation slavery, each creating organic food (for example) easily accommodated in the same universe. We can get our agricultural produce, our manufactured goods, our oil, knowing what it is, where it came from, that it is “true” and has remained true, without having to police its production. Rather than a center that has to “see” everything, blockchain institutes a world where the fringes of the network – the moment when what we imagine to be material is recorded with its digital double – are the crucial places in it.

Second, blockchain allows other sorts of computational agents to start doing various kinds of work. One area of development is in so-called smart contracts. A smart contract is a distributed application, executable code in a blockchain. When certain changes in state in the physical or digital world meet certain predetermined requirements, the code runs. For example, when sensors confirm that the temperature in a shipping container has been maintained at a predetermined constant without interruption from Time A to Time B, and the shipping container has arrived in port, and a commodity price reaches a certain level, and a corporate account has the required reserve, a smart contract can issue a payment or transfer title without the intervention of any human or institutional intermediary.

Heralding automaticity does not of course mean the liberation of human labor. It raises twinned questions tied to the history of accounting: what happens to the abjected human whose physical labor is obviated by technologies of automaticity or to global, racial, and gendered hierarchies of human labor when some machines run smarter than others? And what happens to the new computational agents, presumably getting “smarter” themselves as they learn from their data-rich environments, and operating as legal actors? Listening to some of its most starry-eyed proponents, I often wonder whether blockchain might institute both human and computational slavery as part of the distributed universe of economic plurality. For me, blockchain occasions speculative fantasies about future heterogeneous human/computational economies.

Just science fiction, I know. But then: how, future archaeologist, are you conducting your work, through what human-computer agencies, and with what attendant or squashed liberties?

Acknowledgments

Research was supported by grants from the US National Science Foundation, Law and Social Sciences program (SES 1455859 and SES 0960423). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. I would like to thank the editors for the invitation to contribute this chapter as well as for comments on earlier drafts. I would also like to thank my colleagues who are also working on blockchain and allied systems, particularly Quinn DuPont, Lana Swartz, Taylor Nelms, Elizabeth Ferry, Peter Graif, and Gretchen Bakke. Special thanks to Jenny Fan, Farah Qureshi, Melissa Wrapp, Nathan Dobson, and Nima Yolmo for research assistance along the way.

Note

- 1 Satoshi Nakamoto. 2009. Original code for Bitcoin. The code is at present maintained on GitHub, a web-based hosting site for code developers to share and maintain version control over computer code, by Leo Trottier, whose “original-bitcoin” repository is “a historical repository of Satoshi Nakamoto’s original bitcoin sourcecode.” Available at <https://github.com/trottier/original-bitcoin>, last accessed 8 October 2018.

References cited

- Agarwal, Arun. 2003. Sustainable Governance of Common Pool Resources: Contexts, Methods, and Politics. *Annual Review of Anthropology* 32: 243–262.
- Aho, James. 2006. *Confession and Bookkeeping: The Religious, Moral, and Rhetorical Roots of Modern Accounting*. Albany, NY: SUNY Press.
- Baucom, Ian. 2005. *Specters of the Atlantic: Finance Capital, Slavery, and the Philosophy of History*. Durham, NC: Duke University Press.
- Baym, Nancy, Lana Swartz, and Andrea Alarcon. 2019. Convening Technologies: Blockchain and the Music Industry. *International Journal of Communication* 13: 402–421.
- Bell, Joshua A., and Joel C. Kuipers, eds. 2018. *Linguistic and Material Intimacies of Cell Phones*. New York: Routledge.
- Benjamin, Walter. 1936 [2008]. *The Work of Art in the Age of Mechanical Reproduction*. New York: Penguin.
- Blanchette, Jean-Francois. 2012. *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents*. Cambridge, MA: MIT Press.
- Brunton, Finn. 2017. Notes from /Dev/Null. *Internet Histories* 1(1–2): 138–145.
- . 2019. *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency*. Princeton, NJ: Princeton University Press.
- Dallin, S. 2017. Cryptocurrencies as Market Singularities: The Strange Case of Bitcoin. *Journal of Cultural Economy* 10(5): 462–473.
- Digiconomist. 2017. Bitcoin’s Energy Consumption Surpasses Ireland. *Digiconomist*, 14 November. Available at: <https://digiconomist.net/bitcoin-energy-consumption-surpasses-ireland>, last accessed 26 January 2019.
- Dourish, Paul. 2017. *The Stuff of Bits: An Essay on the Materialities of Information*. Cambridge, MA: MIT Press.
- DuPont, Quinn. 2018. *Cryptocurrencies and Blockchains*. London: Polity.
- Dwork, Cynthia, and Moni Naor. 1993. Pricing via Processing or Combatting Junk Mail. In: E.F. Brickell (ed.), *Advances in Cryptology – CRYPTO’92*. Lecture Notes in Computer Science, vol. 740. Berlin, Heidelberg: Springer, 139–147.
- Errington, Shelly. 1998. *The Death of Authentic Primitive Art and Other Tales of Progress*. Berkeley: University of California Press.
- Feria, Inês. 2019. Trust, Reputation and Ambiguous Freedoms: Financial Institutions and Subversive Libertarians Navigating Blockchain, Markets, and Regulation. *Journal of Cultural Economy* 12.
- Ferry, Elizabeth. 2016. On not Being a Sign: Gold’s Semiotic Claims. *Signs and Society* 4(1): 57–79.
- Foster, Robert. 1999. In God We Trust? The Legitimacy of Melanesian Currencies. In: David Akins and Joel Robbins (eds.), *Money and Modernity: State and Local Currencies in Melanesia*. Pittsburgh, PA: University of Pittsburgh Press, 214–231.

- Future of Money Research Collaborative. 2018. Social Payments: Innovation, Trust, Bitcoin, and the Sharing Economy. *Theory, Culture and Society* 35(3): 13–33.
- Geismar, Haidy. 2013. *Treasured Possessions: Indigenous Interventions into Cultural and Intellectual Property*. Durham, NC: Duke University Press.
- Golumbia, David. 2016. *The Politics of Bitcoin: Software as Right-Wing Extremism*. Minneapolis, MN: University of Minnesota Press.
- Gregory, C.A. 1996. Cowries and Conquest: Towards a Subalternate Quality Theory of Money. *Comparative Studies in Society and History* 38(2): 195–217.
- Hardin, Garrett. 1968. The Tragedy of the Commons. *Science, New Series* 162(3859): 1243–1248, 13 December.
- Hayek, F.A. 1976. *The Denationalization of Money*. London: Institute of Economic Affairs.
- Karpik, Lucien. 2010. *Valuing the Unique: The Economics of Singularities*. Princeton, NJ: Princeton University Press.
- Lustig, Caitie, and Bonnie Nardi. 2015. *Algorithmic Authority: The Case of Bitcoin*. IEEE Computer Society, presented at the 48th Hawaii International Conference on System Sciences, Kauai. doi:10.1109/HICSS.2015.95.
- Maurer, Bill. 2016. Re-Risking in Real Time: On Possible Futures for Finance After the Blockchain. *Behemoth* 9(2). doi:10.6094/behemoth.2016.9.2.917.
- . 2017. Money as Token and Money as Record in Distributed Accounts. In: N.J. Enfield and Paul Kockelman (eds.), *Distributed Agency*. Oxford: Oxford University Press.
- . 2018. Primitive and Nonmetallic Money. In: S. Battilossi, Y. Cassis, and K. Yago (eds.), *Handbook of the History of Money and Currency*. Singapore: Springer. doi:10.1007/978-981-10-0622-7_2-1.
- . 2020. The Politics of Token Economics, Then and Now. In: A. Crisà A., M. Gikaki, and C. Rowan (eds.), *Tokens: Culture, Connections, Communities*. London: Royal Numismatic Society, 215–229.
- Maurer, Bill, Taylor Nelms, and Lana Swartz. 2013. ‘When Perhaps the Real Problem Is Money Itself!’ The Practical Materiality of Bitcoin. *Social Semiotics* 23(2): 261–277.
- Medley, Bill. 2014. *Highways of Commerce: Central Banking and the US Payments System*. Kansas City: Federal Reserve Bank of Kansas City.
- Myers, Fred. 2002. *Painting Culture: The Making of an Aboriginal High Art*. Durham, NC: Duke University Press.
- Miller, Mark S., and K. Eric Drexler. 1988. Incentive Engineering: For Computational Resource Management. In: Bernardo Huberman (ed.), *The Ecology of Computation*. North-Holland: Elsevier Science Publishers.
- Nakamoto, S. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: <https://bitcoin.org/bitcoin.pdf>, last accessed 26 January 2019.
- Nelms, Taylor. 2015. ‘Ecuador Bans Bitcoin!’ A Monetary Mixup. *The King’s Review*, 20 October. Available at <http://kingsreview.co.uk/articles/ecuador-bans-bitcoin-a-monetary-mix-up/>, last accessed 26 January 2019.
- Poovey, Mary. 1998. *A History of the Modern Fact*. Chicago: University of Chicago Press.
- Price, Sally. 2002. *Primitive Art in Civilized Places*. Chicago: University of Chicago Press.
- Shell, Marc. 1978 [1993]. *The Economy of Literature*. Baltimore, MD: Johns Hopkins University Press.
- Strathern, Marilyn. 1975. *No Money on Our Skins*. Canberra: New Guinea Research Unit, Australian National University.
- . 2013. *Learning to See in Melanesia*. Chicago: HAU Books.

- Swartz, Lana. 2018. What Was Bitcoin, What Will It Be? The Technoeconomic Imaginaries of a New Money Technology. *Cultural Studies* 32(4): 623–650.
- Torpey, Kyle. 2015. Andreas Antonopoulos: Bitcoin Terminology Is Completely Broken. *Inside Bitcoins*, 2 September. Available at <https://insidebitcoins.com/news/andreas-antonopoulos-bitcoin-terminology-is-completely-broken/34641>, last accessed 1 December 2018.
- Zimmer, Zac. 2017. Bitcoin and Potosí Silver: Historical Perspectives on Cryptocurrency. *Technology and Culture* 58(2): 307–334.

Digital Anthropology

Edited by Haidy Geismar and Hannah Knox

Second Edition



Digital Anthropology, 2nd Edition explores how human and digital can be explored in relation to one another within issues as diverse as social media use, virtual worlds, hacking, quantified self, blockchain, digital environmentalism and digital representation. The book challenges the prevailing moral universal of "the digital age" by exploring emergent anxieties about the global spread of new technological forms, the cultural qualities of digital experience, critically examining the intersection of the digital to new concepts and practices across a wide range of fields from design to politics.

In this fully revised edition, *Digital Anthropology* reveals how the intense scrutiny of ethnography can overturn assumptions about the impact of digital culture and reveal its profound consequences for everyday life around the world. Combining case studies with theoretical discussion in an engaging style that conveys a passion for new frontiers of enquiry within anthropological study, this will be essential reading for students and scholars interested in theory of anthropology, media and information studies, communication studies and sociology. With a brand-new Introduction from editors Haidy Geismar and Hannah Knox, as well as an abridged version of the original Introduction by Heather Horst and Daniel Miller, in conjunction with new chapters on hacking and digitizing environments, amongst others, and fully revised chapters throughout, this will bring the field-defining overview of digital anthropology fully up to date.

Haidy Geismar is Professor of Anthropology at UCL, UK.

Hannah Knox is Associate Professor of Anthropology at UCL, UK.

ANTHROPOLOGY

Cover image: © vms / Getty Images



Routledge

Taylor & Francis Group

www.routledge.com

Routledge titles are available as eBook editions in a range of digital formats

an informa business

ISBN 978-1-350-07884-0



9 781350 078840