Title
Blockchains are a Diamond’s Best Friend: Zelizer for the Bitcoin Moment

Permalink
https://escholarship.org/uc/item/22w2n6c8

ISBN
9781400885268

Author
Maurer, WM

Publication Date
2017

Peer reviewed
Money Talks

EXPLAINING HOW MONEY REALLY WORKS

Edited by Nina Bandelj, Frederick F. Wherry, & Viviana A. Zelizer

PRINCETON UNIVERSITY PRESS
PRINCETON & LONDON
To the Princeton University Sociology Department,
where it all started.
CONTENTS

Preface ii
Acknowledgments ixi

INTRODUCTION
Advancing Money Talks
Nina Bandeli, Frederick F. Wherry,
and Viviana A. Zelizer

PART I
BEYOND FUNDABILITY

CHAPTER 1
Economics and the Social Meaning of Money
Jonathan Morduch

CHAPTER 2
Morals and Emotions of Money
Nina Bandeli, Tyler Boston, Julia Elgadhar, Julie
Kim, Michael Melbrie, Zazha Tufail, and James
Owen Weatherall

CHAPTER 3
How Relational Accounting Matters
Frederick F. Wherry

PART II
BEYOND SPECIAL MONEIES

CHAPTER 4
The Social Meaning of Credit, Value, and Finance
Bruce G. Carruthers

CHAPTER 5
From Industrial Money to Generalized Capitalization
Simone Polillo

PART III
CREATING MONEY

CHAPTER 6
The Constitutional Approach to Money: Monetary
Design and the Production of the Modern World
Christine Desan

[ vili ]
<table>
<thead>
<tr>
<th>CHAPTER 7</th>
<th>The Market Mirage</th>
<th>137</th>
</tr>
</thead>
<tbody>
<tr>
<td>David Singh Grewal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 8</th>
<th>The Macro-Social Meaning of Money: From Territorial Currencies to Global Money</th>
<th>145</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eric Helleiner</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART IV</th>
<th>CONTESTED MONEY</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Arlie Hochschild</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 10</th>
<th>Paid to Donate: Egg Donors, Sperm Donors, and Gendered Experiences of Bodily Commodification</th>
<th>177</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rene Almeling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 11</th>
<th>Money and Family Relationships: The Geography of Transnational Money</th>
<th>184</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sapriga Singh</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART V</th>
<th>MONEY FUTURES</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 12</th>
<th>Money Talks, Plastic Money Tattles: The New Sociability of Money</th>
<th>201</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aija Gurvica and Azos Ruma-Tau</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 13</th>
<th>Blockchains Are a Diamond's Best Friend: Zelizer for the Bitcoin Moment</th>
<th>213</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bill Mauer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 14</th>
<th>Utopian Monies: Complementary Currencies, Bitcoin, and the Social Life of Money</th>
<th>230</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nigel Dodd</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Selected References on the Social Scientific Study of Money | 243 |

| Contributor Biographies | 255 |

| Index | 261 |
Blockchains Are a Diamond’s Best Friend

ZELIZER FOR THE BITCOIN MOMENT

Bill Maurer

VENMO. LEVELUP. APPLE PAY. SQUARE. In ten years’ time we will see which, if any, of these new electronic payment providers still exist, much less capture the kind of market share enjoyed by that most venerable of digital payment devices, the plastic card. At the time of my writing, there is an unprecedented proliferation of new payment technologies and a pace of innovation not seen before in the history of ways to separate people from their money, quickly, conveniently, and reliably. Scott Mainwaring, an industry researcher, has termed it a “Cambrian explosion in payments”: a blossoming of myriad technologies, using different platforms, devices, and networks, to help people pay (Deville 2014; Maurer and Swartz 2015). Where the payment card networks originated in retail store credit and later, associations of banks sharing communications networks for clearing and settlement, the new systems rely on a variety of infrastructures: mobile telecommunication, the Internet, distributed peer-to-peer networks. They harness features of new digital and mobile-computing devices not originally designed to support payment, such as the digital camera and display screen (for optical recognition and transmission of payment information between a person’s device and a point-of-sale terminal, in the case of LevelUp) or the headphone jack (for input of payment data from the magnetic stripe on the back of a traditional magnetic stripe card, is the case of Square). It is a Cambrian explosion in that new body forms, adaptations of existing structures, and novel relationships in a variegating ecology of retail payment are coming into being all at once, radiating
out into a landscape hitherto the exclusive preserve of paper banknotes, coins, and plastic cards.

If The Social Meaning of Money were written today, Viviana Zelizer would have to account for these new technologies. Indeed, they beautifully make the case she put forward: these are socially differentiated and differentiating ways of paying that render the monies associated with them similarly multiple. Different groups gravitate toward different payment technologies: teenagers and college-age students today are the near-exclusive users of Venmo, a micropayment service that integrates with social media so that users can see each other's payment activity. Early adopters of Bitcoin, an experiment in cryptographic currency, were almost exclusively white, male, hard-core programmers, with a heavy smattering of libertarians. If the Bitcoin community has diversified since then, it is only in its internationalization, especially as Chinese adherents trade in the currency despite their government's efforts to crack down against it. Apple's mobile payment service, Apple Pay, is only available to owners of Apple's newer (and more expensive) iPhones, creating a segmented market that itself is further separated from the ho ho ho of commerce because, at least in the early days, Apple Pay was only accepted at select retailers (such as the high-end supermarket chain, Whole Foods). They are socially differentiating, too, in that Venmo, for example, not only reflects but creates circles of friends with whom one shares one's economic activity—a new kind of conspicuous consumption (Tung 2015). Bitcoin facilitated transactions on Silk Road, an online anonymous marketplace for illicit goods and services, until the latter was shut down by authorities in 2013.

While these are, for the most part, new payment infrastructures, and not wholly new monies, the line is blurring. Private companies creating new payment "rails" (as they are termed in the payments industry; see Maurer 2012) are also floating new kinds of value-laden tokens, electronic coupons, and point- or credit-based systems that enter into circulation alongside state-issued money, albeit, for now, in "closed loops"—another industry term referring to the limited redeemability of such tokens. American Express, the charge card company, and Amazon.com, the online retailer, have an agreement allowing the use of Amex's Membership Rewards points for purchases. People taking advantage of this arrangement discuss the ins and outs of the variable exchange rates between points and dollars, and the difference between purchasing directly over Amazon.com with one's Amex card, versus using Amex points. Such arrangements attract regulatory attention, with central bank regulators, among others, worrying about whether they augur the re-emergence of private currencies, or, more prosaically but equally concerning, whether they open new possibilities for money laundering or tax evasion.

If new payment services shade into new monies, they make more complex the already multiple and cross-cutting social relations of money that Zelizer documented. But they may do more. As I will argue, such developments in the Cambrian explosion of payment highlight money itself as money of account. That is to say, they draw attention to, underscore, rely on, and reanimate the unit of account function as the core, distinguishing function of money in general. This is not to suggest that they desocialize money (as perhaps Ingham 2001 would argue) but rather reveal the social meanings of money in its accounting. New payment systems remind us that people's everyday earmarking and queuing of special monies is itself a kind of accounting.

In what follows, I discuss Bitcoin and its underlying technology. Specifically, I address how new uses of that technology shed light on money as money of account. This bolsters the arguments of alternative monetary theorists like Geoffrey Ingham and Randall Wray, which were often seen in opposition to the Zelizer view. Both Zelizer and alternative monetary theorists argued on the paucity of the mainstream economists' take on money as a neutral medium of exchange. Zelizer highlighted its social vagaries. Ingham highlighted money of account, the "means of accounting for value" (2001: 307). Such accounting is always linked to the state's ability to demand taxes paid in its own token and the systems of claims and counterclaims in credit-money that ultimately rely on state's banks' promises to pay (ibid.: 312). Whatever social vagracy may exist, Ingham argued, would still be determined by and deminated in money of account. I ask whether developments like Bitcoin and other forays into new payment services more generally have the potential to open up these relations between states and banks with regard to money.

Bitcoin is also interesting in the universe of electronic forms of payment because of the way it both does and does not "tell tales" of its movements and sociability (see Guseva and Renaux in chapter 12 of this volume). It was designed to be anonymous. But central to its functioning is a publicly available, shared, verifiable ledger, a giant digital record book of all transactions. Bitcoin depends on a chronicle of transactions whose principals' identities are difficult, if not impossible, to ascertain. To its proponents, this is a virtue, and a form of sociability that takes "trust" out of the business of money. As I discuss below, however (and as Nigel Dodd explains in chapter 14 of this volume), the picture is a bit more complex. Understanding how Bitcoin elevates money as money of account helps explain why.

Earmarking and Accounting

There is not as much distance between Zelizer and Ingham as appears at first glance. Earmarking as discussed by Zelizer is nothing but accounting. If Zelizer relegates the state to the background, it is only to reveal more clearly the "everyday practices and meanings of people's money worlds and repertoires" (Goyer 2004; Eggleton and Williams 2007). Zelizer opened The Social Meaning of Money with a plea to move beyond the view of people as rational individuals "making decisions only of price and quantity" (Zelizer 1994: 1997: 4).
She referenced the wonderfully evocative stories of midcentury housewives’ “tin can accounting” and Orange County, California, shoppers’ “stash stashes” for special use” (Ibid.: 5). Listen to one such housewife: I have a silly little system. Whenever my husband gets paid I take away so much for my grocery money and put it in my kitchen drawer. Then I take all the rest and I put it into a tin can. If we can pay a bill in person we take the cash out of the can. . . . Now, whatever is left over in the tin can by the time the next payday comes we transfer into the bank account to pay our future bills. If my husband doesn’t have enough money for gas out of his allowance, or if we go out for some entertainment we just take the money out of the tin can. Sometimes there is only a little left in the tin can at the end of the period, and sometimes there is a lot—it just all depends on the week. (quoted in Rainwater, Coleman, and Handel 1968: 165)

Such stories led Zelizer to excavate how money, presumed to be purely fungible, gets parcelled out into distinct bundles and set to specific uses that open a window into social worlds of meaning and relationality.

Earmarking is an accounts-keeping operation, as Rainwater, Coleman, and Handel point out. Lacking other easy means of keeping track of their money and their expenditures, midcentury housewives found ways materially to segregate and visualize their financial standing and to make savings and purchasing decisions. Their accounts, physically manifested in tin cans, envelopes, or china pitchers, were also a material demonstration of their relationships and values. Other researchers building on Zelizer and citing this and similar studies were able to prove experimentally how people deploy funds and other resources based on implicit and explicit labeling schemes (Heath and Soll 1996).

This kind of research, however, generally aimed to show how such labeling led to misallocations—irrational decisions—rather than to underscore money’s social meanings. Things that are easier to label or categorized end up being the “most subject to the rigors of budgeting” (Heath and Soll 1996: 40). The primary sources on such forms of “mental accounting” also documented that the practice breaks down because, among other things, people using it have a “tendency to ‘cheat a little’” (Rainwater, Coleman, and Handel 1968: 165).

I linger over this material because I think authors in the mental accounting literature actually got something wrong that Zelizer, at least indirectly, got right. Tin can accounting was a form of physically differentiating monies. It was a socio-material practice that embodied social meanings. The aim was not merely to control spending but to give a visceral account, not a mental account, of what people were spending. The practice breaks down because people feel that their account was being cheated. The practice breaks down because people feel that their account was being cheated. The practice breaks down because people feel that their account was being cheated. The practice breaks down because people feel that their account was being cheated.

The accounting system Bitcoin relies on is a distributed database that contains a ledger of all transactions, called the blockchain. Rather than living on one computer or server, the database resides in duplicate form on all of the computers verifying Bitcoin transactions. The second system is a protocol for verifying transactions in that ledger by way of a computationally difficult competition, called a proof-of-work, among parties to the system who are rewarded for their effort. The technical details are challenging (Clark 2013), but the concept is relatively straightforward: Bitcoin is based on a ledger, the blockchain, which exists on all the computers participating in the Bitcoin system (at least in theory, as there are now third-party services that will exchange your bitcoins for you without your having to maintain a copy of the ledger on your own computer). The ledger is continuously updated by the nodes in the network, which are undertaking proof-of-work to verify any new transactions in a kind of computationally intensive lottery. When a node wins the lottery and completes the verification of a set of transactions, a “block” is said to be completed, and it is broadcast to the whole network. The update has to be agreed to by 51 percent of the nodes. This process is called “mining,” and Bitcoin miners who win the competition to complete a block are provided a reward in bitcoins, which provides a mechanism for the introduction of new currency into the economy.
system, but only as far as a predetermined upper limit. Miners can also charge transaction fees.

The blockchain contains entries of all bitcoin transactions. The ledger records the "addresses" of the transacting parties, which are themselves crypto-graphically secured and quasi-anonymous—there is no identifier linking a person’s name, say, to that address. Transactors’ ownership of bitcoins is essentially the right to a ledger entry. In other words, there are no actual tokens or digital ledger ticks. Rather, the ledger contains entries of transactions between addresses. Addresses are secured by a set of cryptographic keys—a public key, from which is computationally derived the public address, and a private key, to be held only by the owner, which is used as the authorizing signature of a transfer of ownership. Hence, "cryptocurrency." One cannot access the bitcoins—that is to say, the proof of the completion of a prior transaction exchanging value denominated in bitcoin—without a private key corresponding to the public key associated with the address containing the record of that prior transaction. If I want to send bitcoin from my address to your address, the Bitcoin protocol distributes my request to send to the entire network, which in turn requires that I authorize the transaction with my private key. If I lose my private key, there is no way to reclaim access to the bitcoin associated with my public address. It becomes locked up in the blockchain forever, or "burned.

No coin, just accounting. No central authority issuing currency. A database containing a ledger maintained through computation, competition, and consensus. These are the basics of the Bitcoin system. But still, as Christine Desan (in chapter 6 of this volume) might say, it is a governance project. It is a digital money of accounts, almost exactly like the captives that so exercised John Maynard Keynes (Ingham 2000), except instead of being "recorded by word of mouth or by book entry on baked bricks or paper documents" (Keynes 1930: 158: 3) it resides in a distributed digital ledger. When Bitcoin began, the rhetoric of mining, the built-in upper limit to the amount of bitcoin ever to be "mined"—that is, a hardlimit on the ultimate size of the ledger—and the antigovernment ideological positions of some adherents lent an anarchist and libertarian character to the system. Bitcoin adherents were like latter-day goldbugs (Mauer, Nelms, and Swartz 2013). Bitcoin’s association with criminal activity over the so-called dark web, Silk Road, and other illicit trading services, and scandals involving several Bitcoin currency exchanges imbued the system with an air of dangerousness, as well as a libertarian political charge. When I attended a payments industry conference in 2013, Bitcoin proponents surreptitiously sifflized stickers and handmade signs to tables and displays in the exhibit hall. People vocally espoused antigovernment, anti-fla t currency and anti-Federal Reserve views (Brunton 2015). At the next year’s meeting of the same conference, however, the exhibit hall was garbed with professional-looking corporate displays, complete with hired female models(!), to promote new Bitcoin start-ups. In 2014, one such start-up announced its sponsorship of the St. Petersburg Bowl, renamed the St. Peters burg Bitcoin Bowl. Football aside, Bitcoin is entering the world of big business. Bitcoin-related venture capital funding approached 8 billion in 2015; it was just above 3 billion in 2014. But it is the blockchain, not the currency itself, that seems to hold appeal outside of Silicon Valley and in the halls of Wall Street, among legacy payment providers (such as Visa or MasterCard), and for the IT departments of regional banks and credit unions. This is because of the blockchain’s essential nature as a database—more precisely, as a distributed ledger. A blockchain is a special kind of ledger. It exists everywhere in the network. There is no one central repository where it resides or one central records keeper. Picture the old ledger books kept in the back rooms or vaults of a bank. Now, imagine a flood, or fire. With a blockchain database, the risk of loss is minimized if not nonexistent, because every node in the network has a copy of the whole ledger and the system is designed so that the nodes in the network continuously update and synchronize those ledgers.

"Now, go back to that dashed ledger book," imagined a bad actor. Someone who through malice, fraud, error, or stupidity makes an incorrect entry. There may be audits, there may be reconciliation of accounts, but the effort to locate the discrepancy may be costly and time-consuming. A core feature of the blockchain as a distributed ledger is that it is public—every node in the network can see it; in fact, everyone in the world can see it, because it is posted online in real time, too. Although it is public, the identities of the transacting parties are concealed by the protocols governing their addresses, as mentioned earlier. These transacting parties do not need to know or trust one another in order to do business; the process of transaction verification through distributed consensus, and the public nature of the blockchain, militates against fraud. At last, militates against fraud once a transaction has entered the blockchain and has been verified: blockchain entries cannot be altered without the consensus of 51 percent of the nodes. Fraud can take place outside the system—I can steal the private key to your Bitcoin address and make off with your money. Or, more simply, I can ask you to send me your credit card number for your participation in a Bitcoin mining scheme and just steal your credit card number. These are not vulnerabilities of the blockchain itself, however, but are external to it.

I have been told personally and have heard public statements to the effect that the "brand" of Bitcoin as a currency is too tainted by the early scandals, criminal investigations, and prosecutions to gain any traction in mainstream legal and financial services sectors. Bitcoin’s association with radical libertarianism has attracted both positive and negative interest—libertarianism in the first decades of the twenty-first-century United States had appeal, especially for elites garnering an ever larger share of the nation’s wealth—nevertheless,
Bitcoin is seen as too controversial for polite corporate strategic planning. But the record-keeping quality of the Bitcoin system is attracting interest among more established financial industry actors. The wholesale financial services industry sees promise in blockchain databases combined with some sort of proof-of-work verification system to facilitate and speed up interbank clearance and settlement, as well as equities and derivatives trading. People say you have to do a "search and replace" in order to get the idea across to higher levels of the organization: replace "Bitcoin" with "blockchain" or "distributed ledger" before you make your pitch.

Why this interest in the blockchain? It is (relatively) immutable—no one can go back and change old entries without everyone seeing what has been done. Such changes have to be agreed to by everyone, so they probably would not "take" anyway. The blockchain therefore provides a verifiable, time-stamped record of transactions. It is also persistent—it lasts even if some of the nodes go dark. It is a historical chronicle—one damn thing after another—that cannot be easily or unilaterally altered. The participating nodes are continuously synchronizing their copies of the database, and thus money does not "move" from point A to point B in the system. Instead, credits and debts simply get updated, everywhere and in near-real time (about ten minutes, on a good day).³

At a conference sponsored by the American Banker trade magazine in July 2013, Rhythe Masters, formerly of J.P. Morgan Chase and at the time CEO of a new blockchain-related start-up, Digital Asset Holdings, declared that the blockchain would solve the problem of "settlement latency"—the amount of time it takes assets like equities changing hands to clear. This is, admittedly, an obscure area, that of the "infrastructures of post-trade processing," as he put it. But the benefits are faster settlement times, which means the ability to make money on otherwise latent assets awaiting clearance—as well as the resilience and, importantly, resistance to cyberattacks that blockchain-based systems display as a result of their distributed nature. She and others at this conference, formally and in the corridors, expressed the view that distributed ledgers would also reduce back-office operations costs. "You can fire your IT department!" said one, informally. Masters more diplomatically put it this way: You will have "no more reconciliation costs—you have to live in the world of financial services to understand the profound implications of that statement." Of course, you do not really fire your IT department, because you need it to set up and maintain the system, and these are difficult systems to develop. But distributed ledgers offer the same promise of automacity as earlier technologies like the assembly line and the computer itself.

As a ledger, though, the blockchain promises still more: the potential to be able to account for everything, since anything can be entered into it, and not just bitcoin transactions. In a seminar at the University of California—Irvine School of Law in 2013, I was outlining the basics of the blockchain when a law professor with expertise in housing finance had an epiphany. If mortgage notes had been entered into something like a blockchain database, he explained, the mortgage settlement mess after the financial crisis of 2008 might not have happened. After all, one of the main problems in addressing the crisis was determining ownership of mortgage paper. Mutual distrust, operational inefficiencies, and outright malfeasance among lenders prevented information sharing. Two years later, at the American Banker conference, said one pastel pastel, "I can't help but to wonder if things would have played out differently with the financial crisis if things like liens were in the blockchain."

A funny thing is happening on the way to the "distributed ledger space," as some are calling this area of potential business opportunity. While leaving aside bitcoin the cryptocurrency, participants are discovering that ledgers are really good for managing and manipulating other things of value. In rediscovering accounts, they are potentially rediscovering money of account. At least some are getting there by way of Zellerian processes of sequestration and earmarking.

Blockchains are a Diamond’s Best Friend

"Don't store your value in a rock, store it in a block." So reads the website of BTCrig.com. The brainchild of Sebastian Neumayer, an MIT engineering PhD, it offers the ability to create a Bitcoin-based novelty item: a ring linked to a Bitcoin address. BTCrig provides the code necessary to design a three-dimensional ring that points toward a Bitcoin address. I can create a Bitcoin address specifically for the purpose of making a ring. I then use the code on the BTCrig website to create a file that can be sent to a 3D printer. I can add my own design elements to the ring plans before printing it out. The printed ring contains a QR code—a matrix bar code, recognizable by applications run on mobile devices with cameras or optical scanning capability—that links to the public Bitcoin address. By scanning the QR code, I or anyone can see how much the ring is worth in bitcoins.

Although tongue in cheek—or maybe not?—the BTCrig project neatly encapsulates a number of assumptions: love can be expressed in terms of monetary value. The wedding ring is a special kind of sequestered value, symbolizing that love, or securing the relationship in which that love presumably flourishes. Yet, as the website and several accompanying online videos demonstrate (hilariously), actual diamond rings can be lost. If lost, the value is lost, too. Or, a ring might look pretty but be fake, holding less value than it would appear to worth at first glance. Or, further, the diamond might have been the product of exploitative practices in a conflict zone, its value tainted by its origins. As one woman actor says in one of the BTCrig’s videos, as she holds a diamond ring back at the hapless suitor, "I don't want blood on my hands!"

Who holds the private key of the value to which a BTCrig points? Well, as with all matters of the heart, this can be negotiated. One of Neumayer's recom-
mendations is to split the private key between the two partners, so that the value sequestered in the blockchain cannot be spent without the consent and participation of each. The BTCringer provides a means of “restricting fungibility,” as Neumayer put it in an interview with me. He reflected on an extreme way to restrict that fungibility: “Instead of putting the bitcoin in an address that the couple controls together, you could send the bitcoin to a burn address where you can show that no one holds the private keys—it’s like throwing the money into the fire—it’s kind of like the proof of burn that a diamond is … You know that someone burned a lot of money to buy the ring, but you’re never going to get the money back again.”

Zellner has taught us not to automatically recoil from the apparent monetization of persons and relations that always seems to entail capitalism but instead to inquire into the social and cultural bases of economic action (Zellner 1985). Some online commentary of the BTCringer project is critical of the idea that you can put a price on love. Others say that only an isolated geek with little understanding of actual human relationships would find it appealing.

But what is most interesting about the BTCringer is its reliance on the blockchain to sequester earmarked value and its use of the blockchain to create a permanent record of a relationship. Neumayer is very explicit on this point: blockchain systems have “the ability to show proof of existence” without having to rely on a third party, while restricting the fungibility of otherwise convertible value. BTCringer creates a special token, in Zellner’s sense, inside the Bitcoin system. Specific techniques can ensure its continued sequestration, like splitting the private key between the two parties to the relation or, more drastically, “burning” the bitcoin. BTCringer also explicitly reminds visitors to its website of the political economy of actual wedding rings, proclaiming, “Support Bitcoin Mining not Diamond Mining.” A large diamond is stolen and cut into smaller stones. A verifiable and unalterable tracking and certification system from the mine to the jewelry store, there is no way to guarantee that a diamond did not originate in a conflict zone or was otherwise unethicaly produced and distributed. So, while at some level a novelty toy, the BTCringer occupies that same family of phenomena as tin can be used for money. Bitcoin can be used for this purpose. This is what the BTCringer also offers. “Social commentary,” Neumayer said, raising awareness of both the monetary basis of many personal relationships, as well as conflict diamonds. At the time of this writing, a very early stage startup, Everledger, is actually trying to do something about conflict diamonds. Everledger is a London-based company that uses the Bitcoin blockchain to identify and track diamonds. Barclays Accelerator invested £185,000 in the company in March 2015, and it has received very favorable press. The idea behind the company is to gather data on diamonds from insurance companies, law enforcement, and diamond producers to create a digital fingerprint for each diamond and store it in the blockchain. This eliminates the problem of conflicting moans and standards of diamond documentation and certification. The digital fingerprint contains enough data to identify a diamond, and the record in the blockchain can track changes in its ownership. The founder, Leanne Kemp, whose background includes both the insurance industry and the jewelry business imagines expanding beyond diamonds to other high value items. As TechCrunch reported, “it’s starting with diamonds, with a view to expanding into all sorts of luxury goods—such as high end watches, designer handbags and fine art—and basically high value items whose provenance might otherwise be reliant on paper certificates and receipts that can easily be lost or tampered with. The blockchain is a distributed public ledger for tracking provenance in a way that’s more robust and accessible than a paper trail” (Lomas 2015).

Here, the blockchain could be used to demonstrate the proof of existence, Neumayer might say, of a relatively nonfungible object of wealth, and thereby provide a chain of documentation of ownership or of provenance. For Everledger, this is of potential interest for the insurance industry. But Everledger also wants to take on diamond trading fraudfully. It is attempting to do so by using the blockchain to record not just proof of existence but a host of data on individual diamonds, with enough detail to be able to identify a diamond of suspicious origin that might come on the market. “If you have a 5 carat diamond, not only do we capture the serial number that’s inscribed on the stone, but most diamonds are described with four Cs (the cut, the clarity etc.). We take [sic] not only those four Cs, we then take the 40 metadata points that make up the diamond … All of the angles and the cuts and the pavilions and all of the crown. And we take all of that, as well as the serial number, as well as the four Cs, and we put all that into the blockchain,” says Kemp (2015). “Say a large diamond is stolen and cut into smaller stones. Its specificity, described by that metadata and recorded in the blockchain, would permit the identification of those smaller gems and their association with the original item. If BTCringer restricts fungibility of otherwise convertible value, creating the equivalent of a precious stone, Everledger provides a way to account for nonfungible things, or, better, a way to enforce their nonfungibility, to forever be able to specify this diamond as distinct from that one.

Leglers, Laundry, and Love

Bitcoin is opening up money to other relations besides those of state and market. If one accepts Bitcoin adherents’ own reflections on the system, its peer-to-peer network structure permits it to operate in its own separate, parallel zone of economy and politics. For true believers, it is governed by its code, not by people or governments. The hard cap on the number of bitcoins ever to exist also removes bitcoin-as-money from the laws of supply and demand, the price mechanisms of the market. This, for some, is a transcendent coin. Of
course, it is shot through with people, ideology, market devices, law, and regulation—there are exchanges, after all, that serve as points of connection between bitcoin and the rest of the world, and these are key sites for regulatory intervention.

To me what is most compelling about Bitcoin is that the blockchain provides an alternative account, quite literally, in the form of a distributed ledger. Despite most Bitcoin proponents’ claims that the currency is completely fungible, it provides this alternative account by constraining fungibility: no one bitcoin is truly the same as another, as each contains the history of its transactions along the way. Each is always earmarked already. Money of account, in Bitcoin, contains within it its individual, socioeconomic history. Even if that history is very, very difficult to read, it is still there, and the fact that it is there is the key to the whole system, ensuring that there is no double spending of the same bitcoin. This is a digital version of physical earmarking. Unlike tin can accounting, however, there can be no cheating, at least not within the blockchain (there can be all kinds of fraud outside the blockchain, as Silk Road and Mt. Gox demonstrated). Everyone who uses the blockchain can continue to use provenance for diamonds to prevent their illicit trade or the concealment of their origins or BTCring’s use to record and solidify a relationship with a split private key or a burn.

Ingham could argue, in 2001, that the ability of money to be laundered proved his case that the social meanings of money as described by Zelizer were secondary to the social relations of banks and states animating the money of account: “The state does not enquire into the meaning of money or differentiate between thirty ‘shills’ or ‘c weaving’s money it pays tax of £250’ (2001): 314). Alternatively, one could convert a bill that had spent much of its life folded up in origami and sequestered from circulation tomorrow to buy a pack of gum; or I could take money from the tin cup earmarked for the rent and use it to buy a birthday present—cheating, as those mid-nineteenth-century housewives did. For Ingham, money’s fungibility works because money’s moneyness is ascribed outside the market, by the state, which cares only about certain relations. All others can evaporate—or be laundered—away (again, see Dessen in chapter 6 of this volume).

The use of the technology underlying Bitcoin may be challenging this assumption. Anything placed in the blockchain is there forever—or for as long as participating nodes keep up the system. It becomes a kind of immovable property: it is not that it cannot be separated from its owner, but rather that it cannot be separated from its history is the blockchain.21 It can never be laundered. It can be used to launder other currencies, however: ill-gotten gains in US dollars can be converted into bitcoin, their origins outside the system available to observers only if the public address can be traced back outside the system to their source. So, one can launder with bitcoin, but one cannot launder bitcoin. This quality of bitcoin led some developers to the concept of “colored coins,” which would be specially marked bitcoin based on particular ownership or transaction histories, precisely to track their origins and pathways. Colored coins make explicit that a bitcoin’s past is always with it, and always visible to anyone who cares to look. It carries its relations along with it—even if it’s hard to know exactly with whom or what it has had those relations.

Bitcoin is also opening to technological change the universe of nonfungible things—paradoxically allowing them to be more easily liquidated by making them more permanent, more indelible. This is Blythe Masters’s point about the potential of the blockchain to reduce settlement latency: if we have a better and faster way to track ownership of equities, or mortgage paper, or diamonds, we can trade more quickly and easily and reduce the amount of time a nonfungible asset just sits idle. We always have proof of its existence, in the ledger. We do not have to chase a paper trail that may have been intentionally obfuscated. The ledger depends on consensus—to alter records, one would need the coordinated participation of 51 percent of the nodes in the network. The blockchain can facilitate trade by providing a permanent, verifiable, secure, and public ledger maintained among untrusted parties or peers. Bitcoin carries forward this notion because it allows special monies and sustains the nonfungibility of value, the moral or social boundaries around different items of worth. So, by supporting nonfungibility and deinstantiation, the blockchain can permit more things, more distinct and different relations, to enter the market. As with the Cambrian explosion in payment, technology here is supporting, not erasing, the social differentiation of monies.

Bitcoin supports Ingham’s position on the centrality of money of account in that it depends on a computationally derived system of record keeping that warrants its own moneyness—forever. It is this feature, and not its cryptoarchist orientations, that is captivating Silicon Valley start-ups and Wall Street investment banks alike, and adding yet another money-form to the Cambrian explosion in payment.

Notes
1. I would like to thank Taylor Nelson, Lana Swartz, Scott Mainwaring, Eric Bowman, and Don Patterson for the ongoing conversations and collaborative research and teaching that have contributed to this chapter. I also thank Nina Bandel, Frederick Wherry, and Viviana Zelizer for their comments and suggestions, and Sebastian Neumayer for his comments to be interviewed for this paper, as well as other researchers participating whose identities are concealed. All errors and inconsistencies are the sole responsibility of the author. Research on Bitcoin and blockchains is supported by the US National Science Foundation (SES 1459319). 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.
2. In keeping with the emerging standard in the Bitcoin community, I capitalize the term to refer to the community, network, system, and infrastructure, but use lowercase to refer to the currency unit (bitcoin).
References


References