Do libertarians dream of electric coins? The material embeddedness of Bitcoin

Henrik Karlstrøm[1]

Abstract

The new, decentralized, anonymous digital currency Bitcoin has in less than three years gone from a proof-of-concept to being traded for about €78 million on a daily basis. Its ascendancy offers up a puzzle for financial regulators and other law enforcers worldwide, while also promising to fulfill the political visions of a group of market-anarchist cryptographers. While it is still a very small economy in absolute terms, Bitcoin also poses some interesting challenges to traditional economic institutions, and is thus an interesting case for economic sociology. Using the notion of material embeddedness, this paper examines the possible implications of a further propagation of Bitcoin. If the currency proves a success, this will have ramifications for a large number of economic institutions, such as the possibility of taxation of untraceable money, the credit economy and interest rates, and international currency control.

Keywords: Bitcoin, virtual currencies, embeddedness, crypto-anarchy, institutions, trust, cryptography, markets

Introduction

"It's not clear if Bitcoin is legal, but there is no company in control and no one to arrest."
- Joshua Davies (2011)

In October 2008, a username on the Cryptography Mailing list posted a white paper detailing the workings of a new peer-to-peer, pseudonymous digital currency called Bitcoin (Nakamoto 2008). The username Satoshi Nakamoto - most probably a pseudonym itself, for one or more persons - posted the code for software that would enable the production and trade of bitcoins[2] in January 2009. At first, it seemed mostly like an interesting novel way to apply certain cryptographic techniques. 1 BTC cost €0.0005, and new ones were introduced rapidly and easily for home computation. By early September 2013, 1 BTC was worth around €100[3] - two hundred thousand times the initial worth. The currency had already been through several cycles of boom and bust (but with a clear upwards general trend), and the market cap of the Bitcoin trade had grown to more than €1.2 billion[4]. Even if this is measly compared to the €3 trillion of more established currencies that is traded daily (Bank for International Settlements 2010), this new currency has received a lot of attention, and is garnering interest from traders, technophiles and utopian anarchists alike. Meanwhile, the creator(s) has disappeared without ever revealing the actual identity behind the moniker of Satoshi Nakamoto.

[1] Ph.D., Department for the Interdisciplinary Study of Culture, Norwegian University of Science and Technology, 7491 Trondheim, Norway. Contact: henrik.karlstrom@ntnu.no, +47 73591765
[2] Shortened to BTC, and written capitalized when speaking of the entire ecosystem and lowercase when speaking of specific instances of the currency
[3] From the Bitcoin exchange Mt.Gox (mtgox.com), read 11.09.2013
[4] Bitcoin Watch (http://www.bitcoinwatch.com/), read 11.09.2013

What is Bitcoin? In short, it is a combination of three already existing phenomena: 1) a "traditional" electronic currency, 2) a security protocol for handling the challenges of anonymous trading, and 3) computer software for implementing these two things. The software consists of a deterministic computer algorithm that takes the place of modern central banks in deciding when and how new money is added to the money supply, and where each user of the Bitcoin software is a node in a decentralized, peer-to-peer network that is responsible for verifying both the creation of new bitcoins and the authenticity of all the transactions in the network.

New bitcoins are created by the software, which releases a block of bitcoins when any node in the network provides a proof for a mathematical problem. It is set to produce a new block every ten minutes, and the problems become more computationally difficult the more nodes there are in the network to maintain this fixed schedule. New bitcoins are far out of reach of the everyday computer user, and are mainly produced in one of six or seven gigantic server farms. The process is known as "mining". Miners receive new bitcoins for free[5], and can then distribute them by buying things or services for them, or simply selling them at a bitcoin exchange. Crucially, no transaction is counted as having taken place before it has been verified by the other nodes in the network.

Outside of the interesting technical features of the currency, Bitcoin represents some challenges to the status quo. Bank regulators scratch their heads as to how to deal with a currency without any form of central control, without anyone to regulate. Internet libertarians celebrate another strike against central government and surveillance culture. Drug dealers and money launderers rejoice in better, more secure business. Currency traders debate whether it constitutes a creative pyramid scheme or something they will soon have to take seriously. The currency's genesis in an online, open-source, anonymous fashion only seems to add to its allure.

The rapid rise (and possible future rapid decline) of Bitcoin constitutes a fascinating opportunity for the social study of money and markets – a near real-time experiment and attempt to upend some of the core institutions and social practices that lie behind the modern market economy. In this article, I will detail some interesting facets of the Bitcoin technology, focusing on its creators' embrace of a libertarian ideology of non-governmental monetary policies and the promise of technology to free us from politics. By paying attention to the way even seemingly ethereal developments are connected to specific material and institutional arrangements – so-called material embeddedness – we can see how the stronger claims of its adherents might

In the following sections, I will discuss the theory of material embeddedness to show how it can be a fruitful concept for examining a superficially non-material technology. I then discuss the methodological challenges of studying new developments in the virtual world of the Internet, before giving some examples of the ways in which Bitcoin is materially embedded, leading to some closing remarks on how keeping an analytical eye on the material embeddedness of market interactions allows us to understand in what way virtual currencies are intimately linked to the institutional setup of the material world.

[5] However, at present a new block requires so much computational power that the cost of electricity for producing new bitcoins is non-trivial.

Embeddedness and how to trace it

Since Bitcoin is at its core an attempt to expand the purview of markets through destabilizing universally adopted state monopolies on the production and verification of currency, I want to analyze it using current sociological theories on the role of markets and their embeddedness in modern economies. It is well established within economic sociology that markets and the economy in general must be seen as embedded in a larger social context, with rules that are mediated by social ties and institutions that are the result of historically contingent developments (Granovetter 1985; Zukin and DiMaggio 1990). Put simply, markets can only exist and work efficiently if a lot of work is put into creating and maintaining them.

This sociological analysis of markets has focused on the way markets tie into existing institutional arrangements. With the operation of markets relying on spoken and unspoken agreements, personal relationships, a reasonable level of trust, formalised rules directing market transactions, lawmakers, industrial backers and so on, the study of market embeddedness has tended to focused on the study of this social context: what types of bonds exist between actors, which informal rules are in place to mediate interaction, who sits where in which institutions (Krippner and Alvarez 2007; Swedberg 1994)? The main idea is that one cannot give a correct picture of markets without considering the way formal and informal networks, government regulation and political institutions shape markets. This means that varying combinations of networks, regulations and institutions will produce different types of markets, a claim that goes against the grain of traditional economic theory (Dobbin 2004). It also poses a plethora of questions to tackle for sociologists, as indeed they have: What institutions created and sustain markets (Fligstein 2001), what networks are the actors involved in (Dimaggio and Louch 1998), what are the rules of engagement (Edelman and Stryker 2005), and where do actors' preferences come from (Bourdieu 2005)?

The embeddedness literature is not without its critics. Some claim that by making too clear demarcations between other social settings and market settings, it fails to actually integrate markets in the social setting, instead keeping it as an entity separate from larger society. Krippner (2001) claims that by focussing on the surrounding context economic sociology has, like the economists it often criticises, taken the market for granted. Gemici (2007) argues that embeddedness as a concept has value as a methodological approach in that it guides scholars towards the ways markets connect to the larger societal context, but that this achievement is also the reason why the embeddedness approach fails to provide an alternative to prevailing economic thought. The market is still a separate sphere from the society is embedded in. This is a conundrum that economic sociology has yet to solve, as witnessed by one recent attempt to tackle the concept (Dale 2011).[6]

Lately, the sociology of finance inspired by theories from science and technology studies has challenged this view of embeddedness, paying closer attention to the material underpinnings of markets and market relations (Muniesa, Millo, and Callon 2007; MacKenzie 2006). The claim is that the problem with embeddedness theory is that the "social context" which the economy is embedded in is poorly defined. Because it can be difficult to define what exactly a social context is, this strand prefers to trace the more easily identifiable *material* linkages between market actors. This means paying attention to the machines, algorithms and other such market devices that make market operations possible: "Emphasis is put […] not on any substantive definition of what "economic"

[6] Indeed, Dale suggests that there might be something to gain from adopting the more Marxian view that society is embedded in the economy rather than the other way around.

should mean" (Muniesa, Millo, & Callon, 2007:3). In addition to the usual market descriptions of supply and demand, the flow of information and the main market actors, Calıskan and Callon list a whole host of objects to include in the description of market matters: "rules and conventions; technical devices; metereological systems; logistical infrastructures; texts; discourses and narratives" (Calıskan & Callon, 2010:3), and so on.

This makes for a very loose definition of what markets actually do. While it covers all the bases, the unwillingness to prioritise factors means there is a risk of losing sight of the more politicised function of markets in modern capitalist democracies, not least related to the often controversial acts of deregulation. The authors concede that "markets delimit and construct a space of confrontation and power struggles", but this space exists only within the market transaction itself, "until the terms of the transaction are peacefully determined by pricing mechanisms" (Calıskan & Callon, 2010:3). In a way, they wish to avoid extrapolating questions of power and politics from the market situation itself.

This perspective has the strength of keeping the focus squarely on the material basis of economic transactions, but it runs the risk of losing sight of the context within which they occur. Fligstein and Dauter, for example, note that "network theorists […] have generally ignored the possible effects of government and law" in market accounts (Fligstein & Dauter, 2007:107). Countering this, empirical investigations in the material markets vein have demonstrated how economic actors have worked to change the regulatory system to accommodate the new options pricing theory (MacKenzie 2006), and while Callon and Calıskan are mainly concerned with the material configurations of markets, they do not reject the notion that these configurations arise within a setting that is socially defined: "empirical analyses of the complex relation between humans and non-humans […] must be encouraged and pursued" (Calıskan & Callon, 2009:393). Similarly, they point out that markets also employ "technical and scientific knowledge […] as well as the competencies and skills embodied in living beings" (Calıskan and Callon 2010:3) in addition to the list of objects mentioned above.

Much of the difference between the STS and economic sociology approaches to markets lies in their focus: the former represents a concern with theories and their material outcomes, embeddedness with theories and their institutional representations. Pinch and Swedberg (2008) argue for a synthesis of these two perspectives, a material embeddedness, which uses material analysis to establish ties that are if not directly part of a "social context", then at least something richer than a simple listing of the techniques involved. In this manner, markets can be understood as socio-technical enactments with room for social and political strategies employed by human actors in market interactions (institutions, habits, morals etc.).

These two strands of theory have a somewhat different focus, but I believe they can provide a useful framework for making legible some of the nuances of the highly complex world of the algorithmic economy. In line with the idea that embeddedness can be traced by examining the material ties between phenomena, exploring the material and social underpinnings of Bitcoin and its promise to make true some of the visions of the libertarian ideologues that were among the first to see the political potential of the decentralized and pseudonymous internet can yield interesting results.

But how to go about exploring something which is so far from being finally settled? Here I will focus on the ideological roots of Bitcoin, with its basis in a specific form of technological libertarianism. By examining the claims of its early adopters as to the function of Bitcoin, taken from various online

archives of messages, I hope to show how the currency is viewed as much of an ideological instrument as it is a practical mode of exchange. In contrast to this, the materially embedded features of the currency, such as its reliance on very specific physical technologies, can point towards an underlying tension within the rhetoric behind Bitcoin.

Methodologically, studying Bitcoin is not an easy task. The phenomenon itself is fairly new, and what studies have been published of it have been of the more technical sort, examining the properties of the network that sustains the currency or testing its pseudo-anonymity. In addition, the people who have been instrumental in developing the standard are either anonymous themselves or have worked through informal channels, preferring to produce proofs-of-concept through self-publishing on blogs and working out technical details on online message boards. This means that, by necessity, many of the sources that appear in this article are to a certain degree non-verifiable in the traditional academic sense – many are from transient web pages rather than published research. While quoting from faceless internet accounts is a less than optimal solution from a research point of view, it is worth noting that the crypto-anarchist community described below actively promotes anonymity and tends to believe that authority should only stem from the strength of arguments.[7]

Virtual money

Before discussing virtual currency, I have to clarify some terms. The socio-technical arrangements that form the basis of any economy mean that markets and money can only be "virtual" in the sense that they are based on electronic media – in this sense, virtual means "mediated by computers". They are intimately linked to material infrastructure, some of which will be covered later. However, this does not mean that virtual money is material in the same way as non-virtual money. This has to do with the institutions that underlie traditional forms of money, and how these are challenged by the particularities of the design of virtual currencies.

Virtual currency can mean a lot of things, and is often used in connection with quite disparate phenomena. One example is the world of complex financial products such as credit default swaps, bonds derivatives and mortgage loan credit ratings, which are virtual in the sense of being financial representations of value that can be traded. Though they are the playground of financial experts and constitute a large portion of the liberalized market for money and financial markets, they ultimately rely on the actions of regulators and central banks. Similarly, the concrete political ramifications of the Bitcoin economy are somewhat different than the ones that are the result of other, more well-known virtual currencies, such as the market for World of Warcraft gold or the semi-autonomous economy of Linden Dollars, the currency in the online virtual world of Second Life (Jin and Bolebruch 2009). While both these virtual currencies facilitate "real-life" economic phenomena such as money laundering or gold-farming (Castronova 2002), the very concept of Bitcoin is more ambitious in its promise to change the way the global economy works.

For the purposes of this article, the term "virtual currency" as it refers to Bitcoin-like schemes means a currency that has the following characteristics, which will be expanded on below: 1) the money supply is managed algorithmically by computer software instead of institutionally by central bankers; 2) supervision of transactions is distributed and non-hierarchical. There is no single authority that can authenticate the money; rather it is done through verification of each transaction by other nodes in the network; 3) the online "wallets" of bitcoins cannot be directly coupled to an offline identity.

[7] See http://lesswrong.com/lw/lx/argument_screens_off_authority/ for a summary of this position

Together, these form the core principles of a successful decentralized, anonymous digital currency, which Bitcoin is believed by some to be the first example of.

Most currencies rely on some sort of centralized control over the supply of money – there is a monopoly on issuing money. This monopoly function is usually performed by the institution of the central bank, which also uses the instrument of interest to manage the rate of inflation due to the general trend of expanding the money supply. The central bank also plays a key role in stabilizing the financial system by acting as so-called "lender of last resort" (Fischer 1999), as well as being the instrument in which "the bulk of domestic payment obligations are finally legally settled" (Johnson et al. 1998). Recalling the discussion of the embeddedness of economic institutions, these functions of the central bank can clearly be identified as embedded within a specific political regime, one which sees state control of currencies as ultimately necessary for their stability, and hence the trust economic actors place in them.

Bitcoin seeks to make do without a lot of the institutions that stabilize traditional currencies. The authors of Bitcoin-like schemes see central banks unfairly imposing control on regimes that are best left out of the purview of the state. This is due both to issues of monetary policies (and the right to taxation) and questions of privacy/anonymity. Rather, they seek to create a currency that can be immune from political manipulation due to its completely distributed design.

There are also other characteristics of traditional money and its digital representation that are often taken for granted, but which make for headaches for those who would replace it with virtual money. For example, when dealing in cash, there is never any doubt as to who holds the money. When a good or service is paid for, the original holder of cash does not hold it anymore. This is different when the only instantiation of the money is in terms of bits. How do you ensure that the money being used is not simply duplicated on some hard drive, ready to be used again when you do not pass your electronic transactions through a trusted third party like Visa or PayPal? The problem of "double spend" is one of the important issues facing virtual currencies with a decentralized ledger that want to become widely adopted.

Similarly, regular bank transactions are usually conducted privately, but between entities that are publicly known. Even the most secretive bank havens must have a way of verifying who each end of a transaction actually are. That is, in most banks it is difficult to have an account without letting the bank know who you are. However, for most privacy-oriented virtual currencies this has to be reversed: the entities must remain anonymous, or the point of the system falls away. This means that there must be a way to verify transactions without relying on the identity of buyer or seller. The solution is to make every single transaction public, and this is hard-wired into most e-currency schemes.

Bitcoin is far from the first type of virtual currency. A number of attempts to create a secure way to handle such have been proposed during the last couple of decades. Cryptographer Nick Szabo came upon the idea of a digital, "unforgeably scarce" resource similar to precious metals in the form of "bit gold"[8], which used complicated algorithmic challenges that required a lot of computational power to solve to generate new bits of e-gold. This is the same procedure that Bitcoin uses. The total amount

[8] See the original proposal here: http://classic-web.archive.org/web/20060329122942/http://unenumerated.blogspot.com/2005/12/bit-gold.html

of Bitcoins is set to cap out at 21 million. While the number itself is a more or less arbitrarily chosen function of the parameters of the block release design of Bitcoin, the point of a cap on the money supply is to avoid the problem of inflation. Similarly, the cryptographer Wei Dai developed a concept called B-money, which proved a feasible way to ensure reliable contract enforcement in a system of complete anonymity and where "the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations" (Dai 1998).

Still, these attempts have so far stranded on some tricky puzzles of how to design a system that is both secure, anonymous and works both offline and online. These problems have to be tackled using a combination of mathematical algorithms and cryptographic regimes, which take the place of human policy makers in supervising the supply of money and arbitrating fairness of exchange. In this sense, it is not hard to see how even a de-institutionalized phenomenon such as Bitcoin relies on a host of protocols, trust (in machine code, in programming team, in the security of the code etc.) and infrastructure to function, and can definitely be said to be materially embedded in pre-existing structures. The question remains, though, why it would be so important to design this currency in the first place. Why isn't traditional money good enough?

Free us from the state

The security of Bitcoin transactions is guaranteed through cryptographic software that ensures that communication between two parts can happen in relatively secure anonymity. The protocol is based on work done by cryptographers since the 1980s to make secure virtual communication possible, useful both for government and for those who wish to avoid government (Joye and Neven 2009). While it can hardly be called a dominating faction within the cryptography community, there has since the beginning been a strong current of libertarian sentiments in the discussions about cryptography (Levy 2001). The free market anarchists in the "cypherpunk" movement have been publishing widely on the need for a securely private way to communicate away from the prying eyes of government, through catchy-named publications such as The Crypto-Anarchist Manifesto[9] and The Cyphernomicon (May 1994). Cypherpunks posit that in a world dominated by electronic modes of communication, the possibilities for anonymity means that the threat of violence diminishes. This is because under proper privately encrypted communication, your online presence cannot be connected to your real-life identity, and you are therefore free from the threat of violent retribution for online transactions.

This movement of sorts might seem esoteric, especially considering that the basic tenets of crypto-anarchism were laid in the late 1980s, long before the general population had internet access and even before the protocols most commonly used today existed. However, the cypherpunk movement was instrumental in defeating early attempts at government control over electronic communications, most notably in the case of the Clipper chip introduced by the United States government with the aim of mandating all telephone companies to escrow their cryptographic keys with a government agency, in effect allowing the government to have access to calls and, with time, other electronic communication. By designing their own cryptography system (the Pretty Good Privacy – PGP – protocol) and mobilizing agencies such as the Electronic Frontier Foundation to the cause, the bill that introduced the Clipper was quickly shelved (Zimmermann 1991).

[9] Available for reading at http://www.activism.net/cypherpunk/crypto-anarchy.html

The cypherpunk movement was not only concerned with safe encryption of data. They were also looking to ways to circumvent the state monopoly on control of the economy's money supply. If the state's capability to tax its citizens is hampered because monetary transfers become untraceable – that is, if the ability to make a claim on the property of other people is reduced – then a major goal of the movement has been reached: "[e]nough money could escape the taxation net of the nation-state so that its abilities to operate effectively will erode" (Delaney and Markey 1996:178). These sentiments are echoed by some of the early adopters of Bitcoin. Nakamoto has stated that "It's very attractive to the libertarian viewpoint if we can explain it properly"[10], and Wei Dai states it even more bluntly: "I hope this is a step toward making crypto-anarchy a practical as well as theoretical possibility" (Dai 1998).

It is important to note that the cypherpunks' support for free-market anarchism is not exclusively cast in terms of a negative freedom from intervention from others, where each is left alone from others' snooping. Even more important is the explicit moral support for markets within economic discourse (Fourcade and Healy 2007). This support takes various forms, from arguing that trade and commerce are civilising factors ("partners in trade do not wage war on each other") via arguments that markets are a necessary condition for freedom in other areas of politics to the current conviction that economic growth is the best (and only?) road to human progress. Fourcade and Healy argue that "[markets] play a powerful moralizing role in practice by defining categories of worth" (Fourcade & Healy, 2007:301).

So much for the ideological basis for virtual currencies, which we can see is already embedded in a large array of concepts and institutional arrangements. It is time to ask what the possible consequences of this new world of virtual currency entails, and to do this by examining the sorts of material linkages it produces. The next section describes some of the ways in which a virtual currency can still be linked to non-virtual institutions and more specific types of materialities. It looks at three questions: First, designing a stable procedure for dealing with the problems of having a transparent yet anonymous transaction regime is something that cryptographers have been pondering since the 1970s, and many believe they have actually achieved it with the invention of Bitcoin. How? Secondly, what sort of markets and market solutions arise out of Bitcoin, and in what way do they differ from current market solutions? Thirdly, what are some of the non-market consequences of a possible wide-spread adoption of Bitcoin? Providing clues to these three questions will go some way towards identifying how virtual currencies are materially embedded.

Bitcoin materiality

One thing that is often lost in the discussion of virtual currencies and private pseudonymity is the amount of non-virtual materiality which is required for these schemes to even have a chance of succeeding. In this section, I will discuss three types of material linkages between Bitcoin and the larger, non-virtual social contexts it operates within. The first is the kind of mathematical-computational procedure that underlies the Bitcoin architecture, the set of cryptographic innovations that makes a technology of such hazy legal status possible. The second deals with the types of economic institutions a development such as Bitcoin is produced by and, in turn, itself produces – decentralized markets, a new type of contractuality and a new monetary politics of

[10] In communications with cypherpunk Hal Finney. Read here http://www.mail-archive.com/cryptography@metzdowd.com/msg10001.html

possible hyper-deflation. The third signifies signify the less economic outcomes of these technical innovations, for example when new online black markets pose a headache for drug law enforcement or when free-market anarchists dream of anonymous systems of "assassination markets" that can replace central state law enforcement altogether (Bell 1997).

Before moving to the discussion of these three outcomes of e-currency technology, it should be noted that Bitcoin relies on the same architecture as the internet itself. The complex chain of technology that has to be in place before even the first Bitcoin transaction can be made is notable: the manufacture of computers, fiber-optic cables and all the other kinds of physically grounded machinery that underlies the wrongly assumed-to-be non-physical internet. This physical infrastructure of Bitcoin is clear, but not unique to virtual currencies. The underlying institutional arrangements are however much more singular, and form a rich tapestry of influences.

Because it relies on a combination of secure, anonymous communication and complex algorithms for production and dispersion of the money supply, Bitcoin cannot be understood without taking into account the importance of the technologies it builds on. For example, the ability to link transactions to specific sources digitally (Merkle 1990), the encryption of data for secure communication (Diffie and Hellman 1976), the possibility of timestamping transactions (Une 2001), the use of algorithmic problems to verify them and many other techniques all build upon existing technologies that were originally developed with other uses in mind.

Taken together, these cryptographic functions make up the technology that is required to construct a crypto-currency of the Bitcoin type, and they have been around since the late 1990s. All of these calculations require a non-trivial amount of computational power, however, and this might explain why it took some time for it to be implemented. That, and the fact that the number of people in the cryptographic community that were interested in thinking about crypto-currencies and also taking the time to write the code to implement it is relatively low. In the words of Nick Szabo: "Myself, Wei Dai, and Hal Finney [the inventor of the proof-of-work scheme that inspired Bitcoin's system] were the only people I know of who liked the idea (or in Dai's case his related idea) enough to pursue it to any significant extent until Nakamoto (assuming Nakamoto is not really Finney or Dai). Only Finney (RPOW) and Nakamoto were motivated enough to actually implement such a scheme."[11]

However, even if the number of people thinking about these issues is small, the underlying protocols of Bitcoin are firmly embedded in both a tradition of thought and a specific set of software commands.

Market embeddedness

While the long debates within economic sociology might seem unrelated to the matter at hand, it has clear implications for two of the core issues at stake with the introduction of virtual currency schemes, namely the question of trust and contract enforcement. With traditional markets – technically sophisticated though they may be – the issue of how to establish trust between actors which act in their own self-interest is solved by having a robust system of third-party regulators, which can arbitrate in case of disputes and enforce sanctions in case of contractual breaches. The unevenness of market interaction posited by economic sociology goes deeper than simply saying that markets differ across national borders or institutional arrangements. If actors cannot know *a priori*

[11] http://unenumerated.blogspot.co.uk/2011/05/bitcoin-what-took-ye-so-long.html

which strategy and institutional structure will lead to an optimal outcome, they must rely on socially anchored scripts and conventions (Beckert 2009) to provide guidance to market procedures. These conventions reduce uncertainty and lend some stability to a fundamentally unstable arrangement, but also pose a specific challenge to accounts of these markets to accurately describe and analyse what is going on in a specific market setting.

In anonymous markets, where there is – at least, theoretically – no way of establishing who the person or persons behind a specific account is, the issue of trust becomes crucial. In fact, Bitcoin is designed to function as a trustless system, where there is no need to place your trust in another human being. As with other things in the e-anarchy world, arbitration and enforcement is left to the machines. It is no wonder, then, that traditional contract enforcers view Bitcoin with skepticism. One of the reasons so much work has been put into solving the complex cryptographic problems of implementing virtual currencies is to ensure secure enforcement of contracts. When both (or more) parties of a transaction are anonymous, non-discriminating machines must take the place of final arbiter between them. However, it is a question whether this is not simply replacing one form of trust – that in other humans and their institutions – with another, based on the supposed infallibility of machine code. In fact, there has already been trouble with the software, with a bug causing the public ledger of all transactions (known as the blockchain) to split in half when an update to the official software was released[12]. The sudden existence of a "fork" in the blockchain required a lot of work by bitcoin miners and the back-end developers of the software, both to fix the solution technically, but also to agree on which of the split blockchains to resume running the transaction verification on.

Another interesting type of institutional embeddedness one might observe if Bitcoin becomes more important is that of shadow versions of existing institutions. Although it is difficult to imagine e-currencies such as Bitcoin making up more than a very small fringe of the total economy, it has the potential to have interesting consequences for some of the core institutions of modern economies. One example is banking. While Bitcoin is not inflationary, it does nothing to change one of the fundamental features of modern capitalism: debt (Graeber 2011; Lazzarato 2012). Two individuals can enter into a lending relationship, even under a decentralized, unregulated system, simply by agreeing to pay an individually agreed interest on the loan[13], implemented by lenders and borrowers meeting in risk-adjusted credit markets (The Wine and Cheese Appreciation Society of Greater London 2013). However decentralized the process is to begin with, in all probability the community of Bitcoin users will at some point find it necessary to work trust into the equation again, and indeed the first Bitcoin banks, lending groups and securities trader service have recently been launched[14].

Also, since rate of creation of bitcoins is constant regardless of demand, it runs the risk of running into deflation. For anyone holding bitcoins in moments of high demand it there is little incentive to sell. When other commodities keep losing value in relation to bitcoins this creates a situation of self-reinforcing deflation. This is the reason some have accused Bitcoin of being an elaborate Ponzi scheme which disproportionately favors early adopters (Barok 2011).

[12] http://bitcoin.org/chainfork.html
[13] This can be handled through peer-to-peer payment schemes such as Ripple (Michelfeit 2011).
[14] At http://www.flexcoin.com/, https://btcjam.com/ and http://torbrokerge7zxgq.onion/, respectively.

What these means for the larger population is still unclear. One of the things Bitcoin proponents extol is the impossibility of taxation in a Bitcoin regime. When peoples' actual financial holdings are impossible to trace, evaluating the actual worth of their assets for the purpose of taxation becomes equally difficult. This multiplies the concerns over tax havens that are already prevalent in modern state economies. Indeed, the European Central Bank (2012) and the US Financial Crimes Enforcement Network (2013) have both issued statements about the new quasi-legal currency.

Social materiality

Bitcoin is growing in popularity as a currency of use, and the number of vendors who accept bitcoins as a method of payment is in the thousands[15]. However, one of the most popular uses of bitcoin for commodities is for anonymised trading in illegal goods (Christin 2013), and most prominent of the sites for such traffic is the Bitcoin-exclusive Silk Road, an online black market that operates in a somewhat different manner from regular web sites.

Silk Road does not carry a regular URL, but is rather a so-called "hidden service", which means it can only be accessed through the Tor anonymity network[16]. Tor (originally The Onion Router, which explains why hidden services have the suffix .onion) operates by bouncing web requests through an encrypted network of servers all over the world, making it near impossible to connect traffic to any specific user. Using this sort of "shadow" internet makes it possible for user to browse sites such as Silk Road, which looks like an Ebay or Amazon for illegal substances, in what for all practical purposes is complete anonymity[17]. Ironically, Silk Road's only point of weakness, so to speak, is in its reliance on one of the older infrastructures of modern society, the postal service. In order to get the drugs, the buyer must provide a post address for the goods to be shipped to. Even if this is done using public key cryptography, there is always the danger of customs officials or an astute postal worker noticing something anomalous with the package.

Bitcoin is also useful for money laundering. As it cannot be traced to the original source and bitcoins can be stored as any other digital medium, the only point of intercept for lawmakers would be in the original bank exchanging of other currencies into BTC. These activities on the side of the law have obvious implications in the sense that they reduce the power of law enforcement and increase the power of those who like to avoid the law. Similarly, changes in the supply and demand of dangerous substances or weaponry can have effects on the consumption of these. However, the question of how Bitcoin is socially embedded can perhaps best be traced by looking at how people are talking about and using Bitcoin in a social context, and the best way to assess these connections in the case of a digital currency is to go online. While it is in no way an exhaustive list, an overview of some of the ways in which this technology has brought people together can be illuminating.

The largest online discussion forum devoted exclusively to Bitcoin, bitcointalk.org, has about 100.000 users. There is a monthly magazine with "several hundreds of thousands" of readers and a Facebook-

[15] https://en.bitcoin.it/wiki/Trade keeps a running list, but does not include vendors of things that are illegal in the US, such as gambling and narcotics.

[16] Because of the "hidden" status of Tor sites, they do not require a legible URL. Silk Road can (as of March 2013) be found at http://silkroadvb5piz3r.onion/.

[17] Theoretically, the encryption used by Tor can be cracked with powerful computers and enough time, but with several layers of encryption this would take at a minimum decades. However, this is part of the reason for the use of the term "pseudonymous".

type social network[18]. An online tipping system has been devised for users of webpages to tip others with small amounts of (micro)bitcoins, and there are about 3.000 bitcoin enthusiasts who have held live gatherings in some 40 cities globally, according to the social meeting web page meetup.com. People create decorative novelty coins with QR codes that point to a specific bitcoin address. While these examples are economically insignificant, all of it adds to the social embeddedness of the currency, which again helps strengthen the trust in the viability of the whole scheme.

Of course, the examples above do not exhaust the questions surrounding the implementation of the Bitcoin architecture. Some of the most serious misgivings have to do with the technical security of the protocol. Due to the nature of how it operates, Bitcoin is being thoroughly scrutinized for security flaws. Even though the Bitcoin architecture has proven to be remarkably resilient to attacks against the code itself (in the words of renowned hacker Dan Kaminsky, "every time I went after the code there was a line that addressed the problem" (Davies 2011)), the system is still not entirely trusted. There are misgivings about the scalability of the increasingly resource-intense and time-consuming verification process of Bitcoin transactions which makes real-time transactions potentially difficult (Karame and Androulaki 2012; Becker et al.). Connected to this are environmental concerns about having computers spend so much processing power simply checking that other computers are not cheating.

Although Bitcoin transactions are encrypted using state-of-the-art encryption methods, the way these are implemented might yield some problems. A decentralized system can be much more difficult to change than a centrally controlled one. This is due to the very (embedded, I might add) nature of peer-to-peer software solutions: either a majority of users have to agree on changes being made, or somehow someone is put in charge of effecting the changes that are good for the majority. A decentralized system such as Wikipedia uses a combination of the two approaches, and of course there are many elements of trust and distrust and issues of seniority involved in the successful administration of such a system (Kittur, Suh, and Chi 2008).

Additionally, it has been shown that someone with the skill and resources to do a triangulation of transaction histories could identify as many as 40 % of end users of Bitcoin (Androulaki et al. 2012; Reid and Harrigan 2011), something which jeopardizes privacy. There is also a problem of Bitcoin theft from unprotected e-wallets (which themselves constitute possible points of security breaches), as well as the issue of "dead" bitcoins, unused coins which are lost due to hardware crashes or simple forgetfulness. These are removed from the Bitcoin economy forever and cannot under the current design be reminted[19].

Conclusion

In this paper, I have argued that keeping an analytical eye on the material embeddedness of market interactions allows us to understand in what way virtual currencies are intimately linked to the institutional setup of the material world, just like non-virtual currencies. Even an effort like Bitcoin, which in its most utopian incarnation promises to free money and the social ties that are associated with it from what is seen as the dysfunctional institutions of modern economies, cannot decouple itself from a whole host of material and institutional issues. Along the way, Bitcoin does threaten to

[18] http://bitcoinmagazine.com/about-us/ and https://www.bitcoinsocially.com, respectively.
[19] Currently, about 64.000 BTC – or about 0,6 % of all bitcoins so far mined – are known to be lost: https://bitcointalk.org/index.php?topic=7253.msg1483219#msg1483219

upset some parts of the reigning order (as witnessed by the frantic worries of narcotics officials over the new drug traffic (Alcantara, Alcantara, and Alcantara 2013)), even if it relies on that very old communications networks, the mail.

While it is too early to say exactly what will come of the rapid development of Bitcoin, the widespread interest in it shows that there might potentially be dynamite in this virtual currency. Whether it is the new form of dealing with money is of course not easy to say, as similar schemes with different technical specifications have popped up and might replace Bitcoin in the near or far future, but it has undoubtedly opened up a new arena for social and technical experimentation, with possible repercussions in as yet unknown spheres. However, the examples from above should provide ample indication that even though Bitcoin proponents hail it as a revolutionary game-changer, there are reasons to believe that the sticky social ties and institutional configurations of today's economic world are not so easily displaced.

Acknowledgements and a small disclaimer

I would like to thank two reviewers at Distinktion for their helpful comments in improving this manuscript, and would like to state that I have purchased a small amount of Bitcoins at some point out of pure curiosity. However, if the Bitcoin proponents described in this article are correct what I have done with them will be rather hard for the reader to figure out.

References

Alcantara, Joel, Joey Alcantara, and Junjoe Alcantara. 2013. "Letters to the Editor." *The Journal of the Canadian Chiropractic Association* 57 (1) (March): 97–8.

Androulaki, Elli, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. 2012. "Evaluating User Privacy in Bitcoin." *IACR Cryptology ePrint Archive* (596).

Bank for International Settlements. 2010. "Triennial Central Bank Survey Report on Global Foreign Exchange Market Activity in 2010."

Barok, Dušan. 2011. "Bitcoin: Financial Privacy in a Transparent Economy."

Becker, Jörg, Dominic Breuker, Tobias Heide, Justus Holler, Hans Peter Rauer, and Rainer Böhme. "The Bitcoin System."

Beckert, Jens. 2009. "The Social Order of Markets." *Theory and Society* 38 (3) (January 27): 245–269.

Bell, Jim, Scientific American, and Assassination Politics. 1997. "Assassination Politics" (April).

Bourdieu, Pierre. 2005. *The Social Structures of the Economy*. Polity Press.

Calıskan, Koray, and Michel Callon. 2009. "Economization, Part 1: Shifting Attention from the Economy Towards Processes of Economization." *Economy and Society* 38 (3) (August): 369–398.

———. 2010. "Economization, Part 2: a Research Programme for the Study of Markets." *Economy and Society* 39 (1) (February): 1–32.

Castronova, Edward. 2002. "On Virtual Economies."

Christin, Nicolas. 2013. “Traveling the Silk Road : A Measurement Analysis of a Large Anonymous Online Marketplace”: 213–223.

Dai, Wei. 1998. “B-money.” http://www.weidai.com/bmoney.txt.

Dale, Gareth. 2011. “Lineages of Embeddedness : On the Antecedents and Successors of a Polanyian Concept.” *Journal of Economics* 70 (2): 306–339.

Davies, Joshua. 2011. “The Crypto-Currency.” *The New Yorker*.

Delaney, Mr, and Mr Markey. 1996. “Encryption, Privacy, and Crypto-Anarchism.” In *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, 165. MIT Press.

Department of the Treasury Financial Crimes Enforcement Network. 2013. “Application of FinCEN ’ s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies”. Vol. 100.

Diffie, W., and M. Hellman. 1976. “New Directions in Cryptography.” *IEEE Transactions on Information Theory* 22 (6) (November): 644–654. doi:10.1109/TIT.1976.1055638.

Dimaggio, Paul, and Hugh Louch. 1998. “Socially Embedded Consumer Transactions : For What Kinds of Purchases Do People Most Often Use Networks ?” *American Sociological Review* 63 (5): 619–637.

Dobbin, Frank. 2004. “Introduction.” In *The Sociology of the Economy*, edited by Frrank Dobbin, 1–26. Sage Publications.

Edelman, Lauren, and Robin Stryker. 2005. “A Sociological Approach to Law and the Economy.” In *The Handbook of Economic Sociology*, edited by Neil Smelser and Richard Swedberg, 2nd ed., 527–551.

European Central Bank. 2012. “Virtual Currency Schemes.”

Fischer, Stanley. 1999. “On the Need for an International Lender of Last Resort.” *The Journal of Economic Perspectives* 13 (4) (October 1): 85–104 CR – Copyright © 1999 American Econom. doi:10.2307/2647014. http://www.jstor.org/stable/2647014.

Fligstein, Neil. 2001. “The Architecture of Markets: An Economic Sociology of Twenty-first-century Capitalist Societies”. Princeton, N.J.: Princeton University Press.

Fligstein, Neil, and Luke Dauter. 2007. “The Sociology of Markets.” *Annual Review of Sociology* 33 (1) (August): 105–128.

Fourcade, Marion, and Kieran Healy. 2007. “Moral Views of Market Society.” *Annual Review of Sociology* 33 (1) (August): 285–311.

Gemici, K. 2007. “Karl Polanyi and the Antinomies of Embeddedness.” *Socio-Economic Review* 6 (1) (December 4): 5–33.

Graeber, David. 2011. “Debt: The First 5,000 Years ” New York: Melville House.

Granovetter, Mark. 1985. “Economic Action and Social Structure: The Problem of Embeddedness.” *American Journal of Sociology* 91 (3): 481–510.

Jin, By Seung-a Annie, and Justin Bolebruch. 2009. “Virtual Commerce (V-Commerce) in Second Life: The Roles of Physical Presence and Brand-Self Connection.” *Journal of Virtual Worlds Research* 2 (4).

Johnson, O.E.G, R.K. Abrams, J-M. Destresse, T. Lybek, N.M. Roberts, and N. Swinburne. 1998. “Payment Systems, Monetary Policy, and the Role of the Central Bank.”

Joye, Marc, and Gregory Neven. 2009. *Identity-based Cryptography*. Vol. 2. IOS Press.

Karame, Ghassan O, and Elli Androulaki. 2012. “Double-Spending Fast Payments in Bitcoin Categories and Subject Descriptors”: 906–917.

Kittur, Aniket, Bongwon Suh, and Ed H Chi. 2008. “Can You Ever Trust a Wiki?: Impacting Perceived Trustworthiness in Wikipedia.” In *Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work*, 477–480. New York, NY, USA: ACM.

Krippner, Greta R. 2001. “The Elusive Market: Embeddedness and the Paradigm of Economic Sociology.” *Sociology The Journal Of The British Sociological Association* 30 (6): 775–810.

Krippner, Greta R., and Anthony S. Alvarez. 2007. “Embeddedness and the Intellectual Projects of Economic Sociology.” *Annual Review of Sociology* 33 (1) (August): 219–240.

Lazzarato, Maurizio. 2012. *The Making of the Indebted Man: An Essay on the Neoliberal Condition*.

Levy, Steven. 2001. *Crypto: How the Code Rebels Beat the Government--Saving Privacy in the Digital Age*. Penguin.

MacKenzie, Donald. 2006. *An Engine, Not a Camera: How Financial Models Shape Markets*. Cambridge, Mass.: MIT Press.

May, Timothy. 1994. “The Cyphernomicon.” http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.txt.

Merkle, RalphC. 1990. “A Certified Digital Signature.” In *Advances in Cryptology — CRYPTO’ 89 Proceedings SE - 21*, edited by Gilles Brassard, 435:218–238. Springer New York.

Michelfeit, Jan. 2011. “Security and Routing in the Ripple Payment Network.”

Muniesa, Fabian, Yuval Millo, and Michel Callon. 2007. “An Introduction to Market Devices.” In *Market Devices*, edited by Michel Callon, Yuval Millo, and Fabian Muniesa, 1–12. Blackwell.

Nakamoto, Satoshi. 2008. “Bitcoin : A Peer-to-Peer Electronic Cash System.”

Pinch, Trevor, and Richard Swedberg, ed. 2008. *Living in a Material World*. *Technology*. MIT Press.

Reid, Fergal, and Martin Harrigan. 2011. “An Analysis of Anonymity in the Bitcoin System.” *2011 IEEE Third Int’l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int'l Conference on Social Computing* (October): 1318–1326.

Swedberg, Richard. 1994. “Markets as Social Structures.” In *The Handbook of Economic Sociology*, edited by N Smelser and R Swedberg, 255–282. Sage Publications.

The Wine and Cheese Appreciation Society of Greater London. 2013. “On, Wikileaks, Bitcoin, Copyleft: Three Critiques of Hacktivism.”

Une, Masashi. 2001. “The Security Evaluation of Time Stamping Schemes: The Present Situation and Studies.”

Zimmermann, Philip. 1991. “Why I Wrote PGP.” http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.

Zukin, Sharon, and Paul DiMaggio. 1990. “Structures of Capital: The Social Organization of the Economy”. Cambridge: Cambridge University Press.