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

Henrik Karlstrøm[1]

Abstract

The new, decentralized, anonymous digital currency Bitcoin has gone from a proof-of-concept to a $1 billion economy in less than three years. 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. What happens to trust and accountability in anonymous financial networks that have no third-party arbiters? And what are the longer material and social consequences of this development? 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 implications 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, electronic currencies, embeddedness, crypto-anarchy, cryptography, trust

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 (which is most probably a pseudonym itself, for one or more persons) posted the code for software that would enable the production and trade of bitcoins (shortened to BTC, and written capitalized when speaking of the entire ecosystem and lowercase when speaking of specific instances of the currency) in January 2009. 1 BTC cost $0.0007, and new ones were introduced rapidly and easily for home computation. It seemed mostly like an interesting novel way to apply certain cryptographic techniques. By early April 2013, 1 BTC was worth upwards of $140[2] - 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 total size of the Bitcoin economy had grown to more than $1.6 billion[3]. Even if this is measly compared to the $4 trillion 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) had 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] From the Bitcoin exchange Mt.Gox (mtgox.com), read 07.04.2013
[3] Bitcoin Watch (http://www.bitcoinwatch.com/), read 07.04.2013

What is Bitcoin? In short, it is a combination of a "traditional" electronic currency, a security protocol and a computer program, where a deterministic computer algorithm 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. This means that initially, anybody could produce bitcoins using a standard home computer. Now, 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[4], 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 fact that the creator(s) of Bitcoin chose to demonstrate the fundamental internet-ness of this development by kick-starting a trillion-dollar economy using only a little computer code while remaining anonymous 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 the history of some of the peculiar facets behind the Bitcoin technology, including its roots in initially unrelated cryptographic discussions and its embrace of libertarian ideology. I show how these very peculiarities both give rise to the hopes of this instance of "virtual money" finally freeing the economy from the constraints of arbitrary politics and, simultaneously, that the project is likely to end up producing the same institutions it seeks to avoid, but with certain material consequences that would most certainly provoke debate.

Embeddedness and how to trace it

"*To know values is to know the meaning of the market*"
- Charles Dow

Since Bitcoin is at its core an attempt to expand the purview of markets through destabilizing universally adopted state monopolies, 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 are not quite as simple to understand as neo-

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

classical economic theory would have it be, easily described through mathematical models with human actors acting in rational, utility-maximizing ways in markets of free association. Rather, it 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).

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)?

Embeddedness is not without its critics. Some claim that 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).[5]

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, and how can it be identified, this strand prefers to trace the material linkages between market actors, machines, algorithms and other such market devices: "Emphasis is put […] not on any substantive definition of what "economic" 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.

[5] 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.

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 and scholars interested in performativity have generally ignored the possible effects of government and law" in market accounts (Fligstein & Dauter, 2007:107). Countering this, empirical investigations in the performativity 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.

Virtual money

"If you are going to deploy electronic coins, why on earth make them expensive to create?"
- Ben Laurie[6]

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. They are intimately linked

[6] http://www.links.org/?p=1164

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 e-money.

Bitcoin is different in nature to the type of "virtual" money that exists in the world of complex financial products such as credit default swaps, bonds derivatives and mortgage loan credit ratings. While these 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 promises – in its own at times very verbal propaganda – to change the way the global economy works. In this sense, it is "real" virtual money.

Even though there is intense debate on the exact nature of money (is it an exchange medium, an expression of purchase power, a medium of capital power or an instantiation of debt relations?), there are some institutions that cannot be separated from the existence of "real" money. Firstly, money is national in character, that is, it is printed and maintained by the institution of the central bank. Second, money is currently considered to be fiat, meaning it is decoupled from the value of any specific natural resource and is rather left to represent nothing but a measure of a certain share of the national economic activity. Thirdly, most currencies rely on a central authority to guarantee the authenticity of the money in circulation.

Of course, in modern economies all three of these facets of money are maintained by central banks, who use the instrument of interest and the size of the money supply to keep the value of money relatively stable (most central banks today are both separate from government policies – although this does not mean they are not political – and steered by a strict goal to limit inflation to a few percent yearly). They also harshly punish forgeries and act as guarantors of the validity of the money people use.

"Real" virtual money, of the kind discussed above, has to make do without a lot of the institutions that stabilize traditional currencies. The main target of attack for most crypto-based currency schemes is the institution of central banks, which the authors of these schemes see as unfairly imposing control on regimes that are best left out of the control of the state. This is due both to issues of monetary policies (and the right to taxation) and questions of privacy/anonymity.

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? The problem of "double spend" is one of the important issues facing e-currencies 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 e-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 e-currency. A number of attempts to create a secure way to handle digital currencies 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"[7], 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 of Bitcoins is set to cap out at 21 million. While the number itself it more or less randomly chosen (Sakamoto never gave an explanation for the number), 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

"It's very attractive to the libertarian viewpoint if we can explain it properly."
- Satoshi Nakamoto[8]

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. 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). Crypto-anarchism posits that in a world dominated by electronic modes

[7] See the original proposal here: http://classic-web.archive.org/web/20060329122942/http://unenumerated.blogspot.com/2005/12/bit-gold.html
[8] In communications with cypherpunk Hal Finney. Read here http://www.mail-archive.com/cryptography@metzdowd.com/msg10001.html
[9] Available for reading at http://www.activism.net/cypherpunk/crypto-anarchy.html

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).

The cyber-privacy anarchist movement was not only concerned with safe encryption of data, though. They were also looking to ways to circumvent the state monopoly on control of the economy's money supply. If the central banks were not at liberty to simply print new money as they wanted, the inevitable boom and busts cycle that made modern capitalism unstable and over time unsustainable would not be possible, or at least have much less impact. Similarly, 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 anti-statist movement has been reached.

It is important to note that the 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 the very foundation of economics in its attempt to discuss the implicit (or explicit) cost of various aspects of life is basically moral: "[Markets] play a powerful moralizing role in practice by defining categories of worth" (Fourcade & Healy, 2007:301).

So much for the ideological basis for crypto-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 completely digital currency can have non-virtual links to institutions and more specific types of materialities. It looks at three questions: 1) 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? 2) What sort of markets and market solutions arise out of Bitcoin, and in what way do they differ from current market solutions? 3) 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 e-currencies are materially embedded.

Bitcoin materiality

"I hope this is a step toward making crypto-anarchy a practical as well as theoretical possibility."
- *Wei Dai* (1998)

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 e-currencies such as Bitcoin and the larger, non-virtual social contexts it operates within. These are what might be called procedural, institutional and – for lack of a better term – social materialities. Procedural materialities are the kind of mathematical-computational procedures that underlie the Bitcoin architecture, the set of cryptographic innovations that makes a technology of such hazy legal status possible. The institutional materialities deal 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 possible hyper-deflation. Social materialities 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 e-currencies. The underlying institutional arrangements are however much more singular, and form a rich tapestry of influences. First, there is the long history of computational design, with exotic-sounding concepts such as hash trees, public key cryptography and proof-of-work algorithms.

Cryptic communications

"Coupling computers with telecommunications […]
To what forms of society could this new technology lead?"
- *David Chaum* (1985)

Because they rely on a combination of secure, anonymous communication and complex algorithms for production and dispersion of the money supply, the history of e-currencies cannot be understood without a history of the field of cryptography. A look at how innovations in cryptography has made it possible to design a new virtual currency that sidesteps the problems mentioned above can give a better appreciation of the type of embeddedness that things like Bitcoin relies on and reproduces.

Cryptographers have been interested in the possibilities of anonymous communication since the dawn of secrecy and espionage, but the type of computerized cryptography we are discussing here came to be in the late 1970s, when the first networked computers began to show promise. While most of cryptography is not especially interested in the features of money *per se*, but rather in how

to set up a technical system for securely verifiable communication, some cryptographers have taken this further than simple curiosity of how this infrastructure might look, and have worked on solving a series of practical problems that stood in the way of its implementation.

A look at a series of cryptographic innovations that address these problems can shed light on the type of computational infrastructure which underlies digital payment schemes. Firstly, in order to be able to link a transaction to a specific source, a way of identifying where that transaction comes from has to be developed. This is done using hash trees, which assign new instances of data a name based on the name of its "parent", the original data (Merkle 1990). This way, it can always be verified which source a particular set of data comes from.

Secondly, a way of ensuring that outsiders cannot read private communication, and especially not the identity of the sender or receiver of transaction, is required. This problem was solved with the invention of public key cryptography (Diffie and Hellman 1976), a method of double-side encryption which functions in the way that a recipient of information publicly gives away the key for encrypting a set of data while keeping private the key for de-encrypting it. That way, anyone can send an unbreakably encrypted message to anyone with a public key, but only the holder of the private key on the other end can de-crypt the message.

Thirdly, a way of establishing when a transaction took place is crucial for determining who has the right to a specific transaction (again, the problem of the double spend rears its head), and as a way of tracing past transactions. Cryptographic timestamping builds on the previous development of hash trees (Une 2001), using the hash of a transaction to run the data through a third party, which verifies the time and sends the data back with an unalterable timestamp.

Fourthly, the problem of double spend is solved through so-called proof of work (POW). POW works in the way that along with every single transaction that is done with the currency, a long tail of data about previous transaction histories and how these specific bits were originally mine follows with it. Determining which transaction comes first in the case of duplicate transaction is a question of which bits have the longest tail of transaction history. Proof-of-work as a way of determining is only useful if the work required takes a lot of computational power to produce while at the same time being easy to verify for other nodes.

This ties into the fifth requirement: being decentralized, a peer-to-peer currency system requires a network of computers running common software to receive and verify all the proofs-of-work and timestamps. It means that every node in a network can act as a server for every other node. This type of network is well-known from technologies like torrent files, which are the main mode of transfer of large files on the internet. In other words, it is the technology most common for digital piracy.

Sixth, the entire scheme is predicated upon strong encryption of data. Without a way of encrypting the data that is sent around in the network, all kinds of interruptive shenanigans may arise, such as falsifying information about timestamps or proofs-of-work. Bitcoin uses the encryption protocol SHA-2, which has yet to be cracked in practice. Of course, there are a whole host of other technical issues that must be solved, which cannot be described in detail here (especially something called

"Byzantine-resilient peer-to-peer replication"[10] – but I'm afraid the details of what this entails are too byzantine for this paper).

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

"The root problem with conventional currency is all the trust that's required to make it work."
- Satoshi Nakamoto[12]

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 decentralized, anonymous e-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.

This is one of the central insights of economic sociology: while economic theories of markets suppose automatic cooperation between actors through the mechanism of supply and demand, it is often the case that informal networks of trust trump pure economic rationality. 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* 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

[10] http://www.gwern.net/Bitcoin%20is%20Worse%20is%20Better
[11] http://unenumerated.blogspot.co.uk/2011/05/bitcoin-what-took-ye-so-long.html
[12] From http://p2pfoundation.net/bitcoin

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 e-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[13]. 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[14], 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[15].

Also, with anti-inflationary mechanisms built into the structure of Bitcoin, it runs the risk of having the opposite effect. The rate of creation of bitcoins is constant regardless of demand, and so for anyone holding them in moments of high demand it makes sense to keep hoarding them, because prices are likely to keep increasing. This creates a situation of hyper-deflation, where other commodities keep losing value in relation to bitcoins, and thus further increasing the incentive to hold on to bitcoins. So far, however, it is not certain whether it will become a commodity in itself, and object of speculation, or whether enough circulation can be achieved for it to become a currency in its own right.

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 taken the trouble of issuing a statement about the new quasi-legal

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

currency that the tech-savvy are up in arms about, still somehow skirting the question of the legality of this new development by choosing to treat like any other foreign 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[16]. However, by far the most popular use of bitcoin for commodities is for anonymised trading in illegal goods, 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[17]. 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[18]. 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. However, bitcoin transactions can be split into any number of miniscule amounts (the currency currently goes to eight decimal places), so the risk is very low. While it is not directly analogous since it does not concern laundering money, the fact that Russian oligarchs with their money placed in Cypriot banks have moved their assets to Bitcoins in the face of new taxation regulations (ruble to BTC transactions tripled in a single day) in the spring of 2013[19] show how troubling it can be for regulators.

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 enjoy it. 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.

---

[16] 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.

[17] 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/.

[18] 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".

[19] http://www.foxbusiness.com/investing/2013/03/22/bitcoin-interest-explodes-as-cyprus-nearly-implodes/

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-type social network[20]. 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.

Other issues

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). 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. In the words of an anonymous Facebook user,

> *"It's worth noting that the whole system assumes SHA-256 -- the bitcoin community says that rolling over to something else is just a matter of introducing a new algo, but in actuality it's not nearly that simple. The protocol has no concept of upgrading to different algos, so it would necessitate a complete overhaul of the […] AND a re-computation/rollover of the entire transaction history."*[21]

, which is a long way of saying that 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;

---

[20] http://bitcoinmagazine.com/about-us/ and https://www.bitcoinsocially.com, respectively.

[21] This quote is sourced from http://www.gwern.net/Bitcoin%20is%20Worse%20is%20Better, which is maintained by another anonymous account. While quoting from faceless internet accounts might seem methodologically dubious, it is worth noting that the crypto-anarchist community actively promotes anonymity and tends to believe that authority should only stem from the strength of arguments (see http://lesswrong.com/lw/lx/argument_screens_off_authority/ for a summary of this position). In the words of gwern, "I am not as interesting as my writings, and in some respect, it should not matter who I am or what I have done".

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[22].

Conclusion

In this paper, I have argued two things. First, that keeping an analytical eye on the material embeddedness of market interactions allows us to understand in what way "virtual" money is intimately linked to the institutional setup of the material world, just like traditional money. Second, that 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, quickly runs into some of the same issues that have plagued money since its inception: indebtedness, unsustainable investment cycles and speculation – none of which is necessarily against the libertarian agenda, of course. Along the way, though, Bitcoin does threaten to 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.

Disclaimer

The reader would be forgiven for wondering whether the author has a stake in the Bitcoin economy himself. Do I own bitcoins? The answer is you'll never know.

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*.

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

[22] 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

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.”

Chaum, David. 1985. “Security Without Identification: Transaction Systems to Make Big Brother Obsolete.” *Communications of the ACM* 28 (10): 1030–1044.

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*.

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.

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*, ed. 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*, ed. Neil Smelser and Richard Swedberg, 527–551. 2nd ed.

European Central Bank. 2012. *Virtual Currency Schemes*.

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).

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*.

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*, ed. 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*, ed. 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, eds. 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*, ed. 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.