Scratch

Cash

Clams

Currency

Shekels

Bucks

The political 'virtual' of an intangible material currency

Dough

Capital

Scrilla

Bills

Paper

Riches

Utrecht University
Faculty of the Humanities
MA New Media & Digital Culture

Supervisor: R. Glas

Month and Year: August 2012

Student: Mark A. Jansen
Student ID: 3637603

Abstract

This paper concerns the open source software project Bitcoin. Bitcoin is often described as virtual cash and this paper asks what the term ‘virtual’ signifies when applied to ‘cash’ and in turn what ‘virtual cash’ says about Bitcoin. Bitcoin is related to the 1990s activist movement of libertarian cryptographers known as ‘cypherpunks’ and to the cyber-libertarian political philosophy, demonstrating the historical intertwining of cryptography and politics. Cypherpunks argued that privacy is a prerequisite for an open society and that cryptography and anonymous transaction systems were needed as assurance. Bitcoin is the latest effort by cryptographers to create digital tokens similar to cash, where Bitcoin’s designer Nakamoto argues that with Bitcoin users no longer have to trust a third party, traditionally the bank. Bitcoin does not fulfill this promise as trust remains to be established, albeit in a different manner. Power is not destroyed, but transferred from banks to Bitcoin’s protocol. The paper concludes that ‘virtual’ refers to Bitcoin’s model of how cash appears to function in everyday exchange, allowing user privacy. Bitcoin does not model another aspect of cash, namely that it is a credential referring to debt. Bitcoin discontinues the concept of debt.

Keywords

bitcoin, crypto-currency, cryptography, virtual cash, cybercash, electronic payments, online payments

Personal introduction

In 2008 I was studying in the USA when the financial crisis struck Wall Street and quickly spread to Main Street and beyond. This financial crisis made me acknowledge that I did not know much about money, perhaps besides that it 'is all about the money'. The torrent of messages predicting doom and destruction about an economy crashing to standstill triggered the impression of money as operating system (OS) of our society. As a computing metaphor, the money system is an important process running mostly in the background, much like the many software processes running in the background of the computer on which I type this thesis. This background process suddenly came to the fore, much like when you are in a train station and want to check departure times on your smartphone, counting on its mobile Internet connection and then awkwardly realizing that it does not connect. You notice technology more when it does not work than when it does. For all people currently alive, money has just always been there, not purposively hidden but not drawing much attention either. Now it had drawn my attention, I wanted to know more about its connection lost.

So I started reading books such as *The Future of Money* by former banker Bernard Lietaer, who argues that money is society's central *information system*. At that time I found this literally unbelievable, as I was among the many who hold the wrong belief that there is something of value 'backing' the numbers in our bank accounts and the cash in our wallets. It could not be that our money is 'just' information, could it? It turned out that things are not that simple. Reading various histories of money such as *Debt: The First 5.000 Years*, written by anthropologist Graeber, yielded the insight that our contemporary money provides information about debt. Money is not only capable of expressing a debt *in* abstract numbers, but the money itself is also created *as* debt through loans, all of which administered by banks. In other words, no money without debt and vice versa. I took Lietaer's statement of money as information system with me as I moved from Groningen to Utrecht, discontinuing international business studies for the new media & digital culture master program in Utrecht.

Although I appreciated the experience offered by the diverse courses of this program, I noticed that it did not devote much attention to this one medium; money. I found this rather puzzling as even the discipline of economics conventionally describes money as the *medium* of exchange. Furthermore, I learned that Marshall McLuhan, the well-known 'prophet of the electronic age', in his book

Understanding Media had included a chapter about money. Furthermore, as Douglas M. Rushkoff recently finished his PhD-thesis in Utrecht, I had the opportunity to read his *Monopoly Moneys* in which he analyzed corporatism and criticized contemporary money. Evoking what in the Netherlands is called 'a feast of recognition', it was good to know that also in more recent times there were more who approached money as medium. Furthermore, crisis or not, in virtual worlds like World of Warcraft something profoundly important is happening. Here, people spend time to obtain 'virtual items', like 'gold', exchanging these for what is often called 'real' money like Euro's. Are these people not in their right minds, or might it be that so-called 'real' money is not that much different form 'virtual gold'? Then I heard about the new medium *Bitcoin*, positioned as 'virtual' cash. Ironically perhaps, this project was launched in the same year the financial crisis struck. Bitcoin was my way into money as medium and this thesis is an account of my voyage which reminded me of the movie *Jerry Maguire*, when the client of actor Tom Cruise asks him to scream out loud: "Show me the ~~money~~ Bitcoin!".

Acknowledgements

I express thanks to René Glas for supervising this thesis. Furthermore, although neither cash nor Bitcoins were involved, the intangible credits for designing the frontpage of this thesis really are for Jan Zoutendijk.

Table of Content

1. Introduction

In 2008 the world witnessed the introduction of Bitcoin, an open source software project using peer-to-peer (p2p) and cryptographic software technology. While Bitcoin originates outside the traditional banking system, the software is positioned as a distributed global payments system (Nakamoto, 2008). Around the same time in 2008, a crisis struck the contemporary banking system in the USA, quickly growing into a global crisis. Many banks were 'bailed out' by governments around the world in order to restore trust and prevent the problems resulting from catastrophous cascading failures elsewhere in the banking system in case these banks would fail[1]. These developments led the well-known sociologist Manual Castells to establish the *Aftermath Project*, a research program of intellectuals who "…share the idea that this crisis is not just a financial and economic crisis, but also a social crisis, which is bringing about a fundamental transformation of societies at large." (Aftermath Project, 2012)[2]. Currently, several southern-European countries such as Spain, Portugal and Italy are experiencing difficulties getting government finances in order[3]. Bitcoin arrives in a time of financial unrest when money and banking have become the subject of debate.

Among the arguments put forward in favor of Bitcoin is that there is no possible censorship of who you are allowed to send money to. Unlike the central banking system, there is no central authority, instead "…managing transactions and issuing money are carried out collectively by the network." (Bitcoin.org, 2012). Interestingly, Bitcoin is often positioned as 'virtual' cash, similar to the tangible 'hard' currency most people carry around in their pockets in everyday life (Wallace, 2011; Cohen, 2011). Since the 1990s, cryptographers have endeavored to engineer systems that guarantee financial privacy by making something similar to cash function over the Internet. None of these initiatives such as DigiCash proved successful in the longer run. Bitcoin this far forms the exception, as it is operable since 2008 and the value of a Bitcoin recently stabilized at an exchange rate of about 5 dollar, following wild speculative

[1] These banks were categorized as system-critical and therefore 'too big to fail'.
[2] In his book *The Future of Money*, former banker Bernard Lietaer's confirms this where his core thesis reads "We are now engaged in a structural shift of the world system… the most important of our economic information systems, our money system, has been ignored as a key leverage point for inducing the necessary and desirable changes." (2001 p. 22).
[3] At the time of this writing there still is uncertainty concerning 'grexit'; a looming bankruptcy by Greece resulting in Greece exiting the Eurozone.

fluctuation in the range between 0,01 and 30 dollar. Bitcoin specifically enjoys interest after it was publicized on well-known technology blogs such as Slashdot. Bitcoin also appeared on the radar of the American Federal Bureau of Investigation (FBI) that dedicated an intelligence report to the project (FBI, 2012). In addition, attention for Bitcoin was fuelled by WikiLeaks when the organization started accepting Bitcoins as donations, following the 'banking blockade'[4].

In the past few years, money itself became the center of attention as people suddenly felt confronted by monetary instability. This experience is perfectly illustrated by the spoof article *U.S. Economy Grinds To Halt As Nation Realizes Money Just A Symbolic, Mutually Shared Illusion* on TheOnion.com which states that "…money is, in fact, just a meaningless and intangible social construct." (2010). Furthermore, this experience has led to a desire for ´more real' money'. The libertarian politician Ron Paul, who served as Representative in the American Senate, consistently refers to 'real' or 'sound' money that would result when the USA would return to the gold standard where cash was 'backed' by gold (Dolland, 2012). Besides an apparent desire for 'more real' money, in these times of financial unrest there is a spike of interest in 'complementary currencies' that could function alongside the fiat currencies tied to nation-states. At the same time, the recently released game *Diablo III* includes a *Real Money Auction House*. In this game players can exchange in-game virtual items for 'real, actual money' via a managed clearing house (Hulsebosch, 2012). Despite the outcry for money that is somehow 'more real', contemporary money still seems very 'real' compared to these 'virtual', in-game currencies.

Money is an important institution in the organization of society. Due to its societal importance and many differing and often conflicting histories that involve politics and power, money invokes strong emotional responses. In addition, it is something about which people hold vastly differing beliefs[5]. Furthermore, various authors explore what money might be like in the Internet sphere. Professor of economics Robert Guttmann in his book *Cybercash: The Coming Era of Electronic Money* stated that "…once money becomes software, the monetary process can be organized in entirely new and varied ways. (Guttmann, 2003 p. 11). Bernard Lietaer in his book *The Future of Money* argues that "Money is

[4] That was held by some as a precedent-setting type of censorship (Poulsen, 2010)
[5] Illustrated by the observation that money is described paradoxically by metaphors of solidity as well as liquidity. We talk about 'hard' currency and in the Netherlands a well-known dictum is that money should 'roll'. On the other hand it is often stated that money 'flows' like water and with 'bubble' we refer to a speculative craze.

modem society's central information system", hinting at the compatibility of money and the Internet (2001, p. 22). Lietaer advocates a societal transition in which he foresees an important role for money. He argues that our current money embeds the values of centralization from the bygone Industrial Age, which should be adjusted and aligned with those of the Information Age (2001, p. 9) [6]. Gutmann discusses the 'digital cash' of the company DigiCash and its cryptographic technology, which is also an important feature of Bitcoin, as the solution to insecurities of the public concerning safety on the Internet (2003, p. 94).

Following earlier efforts such as DigiCash, Bitcoin is an implementation of the vision of money as software. It is a new medium that is presented as being similar to cash, apparently 'virtual' and using cryptography to dispose of the bank as trusted central authority. When a medium is described as 'new', the field of new media studies critically asks how new such a medium is and if it is, in what ways. In other words, what changes and what stays the same? Ultimately, I ask here what it implies that the programmer of Bitcoin and several journalistic commentators choose to describe Bitcoin as 'virtual' cash. Therefore, I will examine the use of the term 'virtual' in relation to Bitcoin, which will involve an analysis of the politicalness of software as well as political aspects of Bitcoin, such as the history of cryptography and the implied need for privacy. Furthermore, since the programmers of Bitcoin position it as an electronic analog of cash, this inquiry will also include a brief analysis of the contemporary money system, the concept of debt that it is based on and the status of cash in this system. The result of this analysis are insights into the similarities but also the discontinuities between contemporary money and Bitcoin.

The reader might note that it is not conventional to approach money as a medium. However, already in 1964 Marshall McLuhan in his book *Understanding Media* included a brief study of money as medium, which included its history and various transformations over time, such as credit, currency and commodity. In 2012, media theorist Douglas M. Rushkoff in his PhD thesis *Monopoly Moneys* followed McLuhan's practice of media ecology in his analysis of corporatism and centralized currency. Media ecology is "…the study of complex communication systems as environments" (Nystrom, 1973). Different from current trends in economic analyses, in this thesis I will approach money as a medium.

[6] Lietaer argues that doing so should lead to an era of 'sustainable abundance'.

In the first chapter I will provide a description of Bitcoin as a phenomenon that uses new media technologies. This review will include an analysis of statements made by Nakamoto in the Bitcoin white-paper. Besides the technicalities of Bitcoin, arguments made in this white-paper also provide insight in the political nature of Bitcoin.

2. Introduction to Bitcoin

In 2008, the mysterious entity 'Satoshi Nakamoto' posted a research paper about a design for a new currency called Bitcoin[7]. Bitcoin is an experimental open source software project, which facilitates the exchange of Bitcoins (BTC)[8]. Bitcoin bypasses the (central) banks by building upon peer-to-peer (p2p), known from file-sharing networks such as BitTorrent. Bitcoin complements rather than replaces the conventional banking system that produces and manages fiat currencies such as the euro and dollar. It is important to note that the idea of complementary currencies is all but new. In 1934 such a system called *WIR (Wirtschaftsring)* was founded in Switzerland. Interestingly, WIR was founded almost 90 years ago as a result of the currency shortages and global financial instability of that time, invoking a sense of *deja vu* looking at the contemporary financial context of Bitcoin[9] [10]. Complementary currencies such as WIR are local efforts and often have the goal of keeping local money local (Ithaca Hours.org, 2012). In contrast, like BitTorrent Bitcoin enjoys global scalability, enabling instant payments to anyone, anytime, anywhere in the world (Bitcoin.org, 2012)[11]. As long as one has an Internet connection, compatible hardware and the open-source software, one can participate and proceed without asking anyone's permission.

Bitcoin is designed to remove the centralized monetary policy crafted by bankers and instead use cryptography to control money creation and transfer by means of distribution. In other words, managing the money supply and transactions are carried out collectively by the network following a protocol. On the P2P Foundation wiki Nakamoto writes about Bitcoin that "It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust." (2012). The following statements by Nakamoto are an attempt at explaining the

[7] Satoshi Nakamoto is the founder of Bitcoin. Not much information is publicly available concerning this identity. The Nakamoto entity has been working on the Bitcoin project since 2007 and ended by 2010. The most recent messages reportedly indicate that Satoshi is "gone for good" (BitcoinStats, 2012)
[8] Bitcoin software is released under the MIT license and hosted at Sourceforge (Bitcoin.org, 2012).
[9] In the context of Bitcoin it is important to note that both of WIR's founders, Zimmermann and Enz, had been influenced by the *libertarian* economist Silvio Gesell.
[10] More known complementary currencies are the Local Exchange Trading Systems (LETS), launched in the 1970s, the Ithaca HOUR launched in 1991 and BerkShares launched in 2006.
[11] Bitcoin is a global phenomenon, different from contemporary money which is tied to nation-states, such as the dollar in case of the United States of America.

raison d'etre of Bitcoin while at the same time exposing the political nature of Bitcoin. Nakamoto argues that:

> *The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve*[12]. (2012 emphasis mine)

Nakamoto continues his argument for Bitcoin by mentioning the need for financial privacy, when (s)he states that "We have to *trust them with our privacy*, trust them not to let identity thieves drain our accounts. Their *massive overhead costs make micropayments impossible*." (p2pfoundaction, 2012 emphasis mine). In the whitepaper that details the design of Bitcoin, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Nakamoto further explains the relevance of Bitcoin as follows:

> *Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. … The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. … These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.* (2008 p. 1 emphasis mine):

If there is one recurring theme present in Nakamoto's statements it is the lack of trust. More specifically, trust is lacking with respect to banks, the contemporary institutions that manage the

[12] With the statement "…waves of credit bubbles with barely a fraction in reserve.", Nakamoto refers to the mechanism of the contemporary practice of fractional reserve banking, of which I will provide a brief introduction in the section called *Contemporary Money System.*

financial system. Nakamoto makes the core motivations for the development of Bitcoin very clear, these being the mistrust of so-called 'big brother' institutions that oversee the financial system, such as Big Banks and Big Governments. Other motivations include the perceived instability of the contemporary fractional reserve banking practice and anxiety of invaded privacy and possible censorship afforded by the contemporary organization[13]. The website Bitcoinme.com puts the arguments in favor of Bitcoin in the following words:

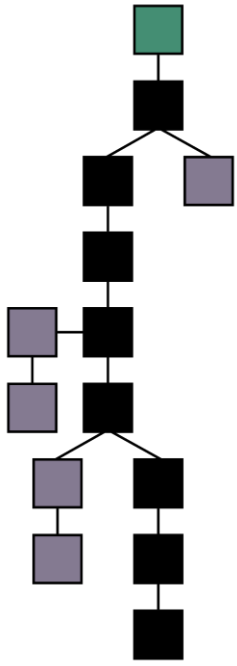
- **Financial privacy**. Does your banker *really* need to know what you buy online?
- **Your account cannot be frozen.** No one can freeze your account and keep your money.
- **No big brother**. Third parties can't prevent or control your transactions. Transfer money easily through the internet, without having to trust middlemen; no central bank, nor central authority.
- **No censorship of who you're allowed to send money to**. No more blocking who you can make payments or donations to... just because someone doesn't agree[14] [15]. (2012)

Nakamoto concludes that "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party." (2008, p. 1). Bitcoin is put forward as the answer to the apparent issues identified above. Nakamoto states that Bitcoin removes the trusted third party and allows users to transact directly with each other. Although a detailed technical analysis of Bitcoin is beyond the scope of this text, to be able to examine Nakamoto's statement I will next provide a basic technical introduction to Bitcoin, in order to familiarize the reader with the Bitcoin protocol [16].

Nakamoto argues that, unlike contemporary currencies such as the euro, Bitcoin has no centralized

[13] In the code of the genesis block, the first block created by Nakamoto, (s)he included the text "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks", intended as proof that the block was created on or after January 3rd, 2009, as well as a hint at the instability caused by fractional-reserve banking practice (Genesis block, 2012).
[14] The last point proved to be a relevant case in point, as of the 'banking blockade' of whistle-blowing organization WikiLeaks in 2011. Here, a consortium of banks at about the same point in time refused to provide financial services to the organization, which made it harder to keep WikiLeaks online.
[15] The FBI has released a report in which they confirm that Bitcoin is very usable in donating to "disreputable groups" and in conducting various activities deemed criminal, such as money laundering (FBI, 2012 p. 10).
[16] For a more elaborate technical analysis I refer the reader to Nakamoto's whitepaper *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008).

authority like a central bank issuing money. This hardly comes as a surprise following that one of the primary goals behind the development of Bitcoin was the by-pass of 3rd party financial institutions that create and manage money. However, this entails that the Bitcoin system has to create money via a different mechanism. This is accomplished through the protocol of the Bitcoin software, where all users that run the software are required to obey a mutually agreed-upon set of rules. In other words, the software has a distributed nature but here the central mechanism is the shared protocol. Via this process Bitcoins are 'verified', popularly referred to as Bitcoin 'mining'. Historically, the software project *bit gold* can be seen as a cryptographic forerunner of Bitcoin. In the article *Bitcoin: Crypto-anarchists' Answer to Cash*, bit gold's programmer Nick Szabo argues in a way similar to Nakamoto that "I was trying to mimic as closely as possible in cyberspace the security and trust characteristics of gold, and chief among those is that it doesn't depend on a trusted central authority," (Peck, 2012).



Nakamoto draws an analogy between Bitcoin 'mining' and gold miners, where (s)he argues that gold miners expend resources to extract gold from a mine and add it into circulation, where with Bitcoin the resources that are expended are CPU- and GPU cycles and electricity (2008 p. 4). The software searches for a solution to a mathematical problem whose difficulty is precisely known[17]. The difficulty is adjusted in an automated fashion, which entails that the number of solutions that are found is constant, approximately 6 solutions per hour (Bitcoin Basics, 2012). When the software on the computer finds a solution, the program distributes the existence of this solution, the 'proof of work' combined with other information, to all other nodes in the

Figure 1. Bitcoin's block chain. The main chain (black) consists of the longest series of blocks from the genesis block (green) to the current block. Orphan blocks (grey) exist outside of the main chain. Source: http://en.wikipedia.org/wiki/File:Blockchain.svg

[17]In this regard, Bitcoin is similar to the @home scientific experiments, such as SETI@home (Search for Extraterrestrial Intelligence), in which one can also participate by running a program that downloads and analyzes radio telescope data using unused CPU cycles. Crucial difference is that the outcome of these calculations is unknown and sought after, whereas in the case of Bitcoin this process functions as an, in principle, unnecessary 'hurdle' where the resulting outcome is irrelevant.

network. This package is called a 'block', which contains 50 new Bitcoins as well as transaction information. The block is awarded to the user that finds the solution, i.e. this user gets new Bitcoins. The award of new Bitcoins for users forms the incentive to participate in this process.

Over time, this process generates a chain of blocks, which is a public record of all transactions involving Bitcoins[18]. Thus, all Bitcoin transaction information, is public, such as transactions value as well as the Bitcoin addresses involved. Here, newly created Bitcoins are regarded as a transaction without a past transaction, i.e. without a source. This public ledger that keeps track of all transactions between Bitcoin users is distributed to, and shared by, the nodes in the network. Through the distributed ledger, the block chain, all transactions in the bitcoin economy are verified through the network and publicly accounted for[19]. Following the current code of the Bitcoin protocol, approximately every four years the number of bitcoins that can be 'mined' reduces by 50%. As a result, the maximum amount of Bitcoins will never surpass 21 million.

The wiki on *Bitcoin.it* states that "The creation of coins must be limited for the currency to have any value." (2012). In other words, the argument is that limiting the amount of something will drive its price up and this idea is implemented by design through code. The incentive to put in the required effort to verify Bitcoins diminishes over time with the decreasing amount of Bitcoins permitted by the protocol. Here the idea is that users who provide the necessary computational power to keep the network running can recoup their investment in hardware and electricity by collecting transaction fees[20] [21]. Although Bitcoins in principle can be send without any transaction costs, the sender of Bitcoins may

[18] The block chain is what enables Bitcoin to solve the 'double-spending problem', that is prevalent in a digital environment in which data are easily copied and possibly 'spend' again. Bitcoin's blockchain acts as a clearinghouse, but one where all users participate and sign off on transactions, instead of one single party acting as central authority.
[19] Via the website blockchain.info one can review charts and statistics concerning Bitcoin, such as the number of transactions per day.
[20] Given that the difficulty of the mathematical problems increases over time, solving them has become practically impossible for the CPU's and GPU's of a single average computer. Therefore, dedicated Bitcoin 'farms' of several computers working together have been set up as investment projects earning Bitcoins.
[21] In addition to the issue of Bitcoin farms holding many CPU's and the rule of one-CPU-one-vote, Victor Grishchenko criticizes Bitcoin's p2p mechanism for not being decentralized, but rather like a 'replicated center' system; "Bitcoin is only "peer-to-peer" in the sense of the British Peerage system. Bitcoin "commoners" must appeal to their "lords" who have sufficient means to judge on validity of transactions and to seal those transactions as valid, likely for a fee." (Grishchenko, 2011)

opt to include a small transaction fee that is awarded to the node that verifies the next block. Paying this fee will provide the incentive to the miner to include the transaction in a block more quickly.

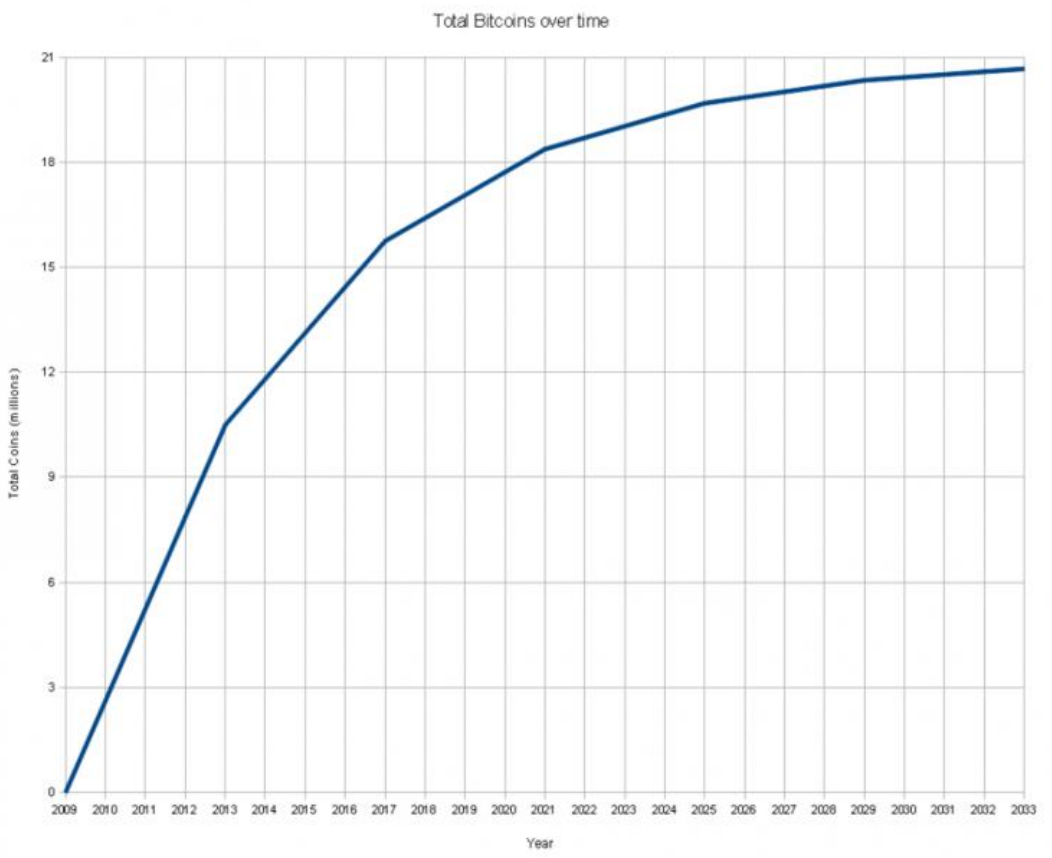


Figure 2. Total Bitcoins over time. Source: http://zh.wikipedia.org/wiki/File:Total_bitcoins_over_time.png

I have stated earlier that Nakamoto is critical of all the trust required by the current banking system, where he proposes that Bitcoin does not require so much trust. Nakamoto argues that a mechanism is needed "…to make payments over a communications channel without a trusted third party." (Nakamoto, 2008 p. 1). Given Nakamoto's desire to remove trust, for Bitcoin a paradoxal key issue is whether trust can be established among the nodes in the network. Nakamoto asserts that "The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes." (2008, p. 1). For the Bitcoin system to work it is absolutely critical that the nodes in the network persistently agree on the state of the database, the block chain, which provides validation.

Control is present and power is established following the political rule that "Proof-of-work is essentially one-CPU-one-vote." (Nakamoto, 2008 p. 3)[22]. The latter rule has important implications for the network politics of Bitcoin, given that the PCs of users participating in the network together keep the network 'honest'. Thus, those with control over more CPU/GPU's command more power [23] [24]. Given the fact that the mathematical difficulty of Bitcoin verification increases as more nodes participate in the process, over time the verification process became a too heavy load for a single CPU or GPU. Therefore, there are now server parks dedicated to the creation of Bitcoins. These are popularly referred to as Bitcoin mining 'farms'.

Figure 3. Photograph of a Bitcoin mining server farm. Source: http://25.media.tumblr.com/tumblr_m3sp4m5Oda1qfy0bho1_1280.jpg

Bitcoin emerged from a lack of trust in existing institutions, but in replacing them Bitcoin shows that it is not possible to somehow 'dispose' of trust, power and control. Trust does not disappear but it shifts from the former intermediary to the next, from bank to Bitcoin's protocol. Bitcoin through its protocol

[22] Organizations commanding great computing power can strive to command 51% of the 'votes', popularly referred to as the '51 percent attack', which would entail that in Nakamoto's term the network becomes 'dishonest'[22] [22].
[23] Although Nakamoto discusses CPUs, in practice certain types of GPU's proved more efficient in Bitcoin mining.
[24] Furthermore, single Bitcoin users controlling one CPU, or a server 'farm', can also further coordinate efforts by combining Bitcoin verification, resulting in 'supernodes'.

functions different from contemporary intermediaries[25]. However, it does not fulfill Nakamoto's promise that with Bitcoin there no longer is a trusted third party, since it remains the intermediating mechanism through which users interact. While a dollar bill states 'In God We Trust', Bitcoin users put their trust in the protocol and its team of contributing developers able to change it[26]. This amongst others entails that users accept the arbitrary limit of 21 million Bitcoins and the one-CPU-one-vote rule.

In the next section I will continue on the political nature of Bitcoin, discussing the historic connection between cryptography and politics and relating Bitcoin to the 1990s privacy movement of cryptographers. In addition, I will argue that Bitcoin resonates with the cyber-libertarian movement from the 1990s. Furthermore, I will show that widespread adoption of Bitcoin poses a challenge to the contemporary method of how governments secure revenue.

3. Privacy, cryptography and libertarianism

The idea of digital cash has been a hot topic since the birth of the Internet, debated intensively by 'cypherpunks', the 1990s movement of libertarian cryptographers[27]. Cryptography comes from Greek κρυπτός meaning 'hidden, secret'; and γράφειν, *graphein*, meaning 'writing'. It is the practice and study of techniques for secure communication in the presence of third parties that are commonly called 'adversaries'. In his book *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*, Stephen Levy explains that cryptography is used when a sender encrypts information into cipher, plaintext into ciphertext[28]. Hereafter, the receiver decrypts the cipher, transforming the apparent disorder back into the original information (Levy, 2001 p. 12). Cypherpunks are activists who make privacy a priority and advocate the use of cryptography as a means to effect social and political change. In the 1990s, cypherpunk grew into a political movement as cryptographers discussed the public policy issues related to cryptography and the politics of concepts such as anonymity, pseudonyms, reputation

[25] In his book *Monopoly Moneys* media theorist Rushkoff argues that the consistent working of a protocol should not lead to the conclusion that any medium is 'neutral'. Instead, no media are neutral but instead all carry structurally embedded biases (2012, p. 22). In other words, outcomes are consistent but consistently skewed. Buying into Bitcoin means to accept its structural bias.
[26] An analysis of how 'open' this team is to new participants in developing and innovating Bitcoin is outside the scope of this text, as is whether their decision making process is in any way 'democratic'. I consider these topics worth researching given network politics and the ability to put forward arguments about how Bitcoin ought to be.
[27] Cypherpunks, derived from 'cipher' and 'punk', was used to describe cyberpunks who used cryptography.
[28] Cipher is a collection of information that for humans appears as unreadable meaningless gibberish.

and privacy. In *A Cypherpunk's Manifesto*, Eric Hughes argues that "Privacy is necessary for an open society in the electronic age. … Privacy in an open society also requires cryptography." (1993).

Bitcoin is often acclaimed for its affordance of anonymity. However, in his book *Code V2* law professor Lawrence Lessig reminds us that in relation to privacy cryptography presents a Janus-face. Here, Lessig quotes cryptography law experts Baker and Hurst, who in their book *The Limits of Trust: Cryptography, Governments, and Electronic Commerce* argue that cryptography will "…make us all anonymous, and it will track our every transaction." (1998). The latter is clearly applicable to Bitcoin due to its public block chain. Cryptography works both ways because encryption can serve two fundamentally different ends, in favor of privacy but also in favor of traceability. Lessig argues that privacy:

> *In its "confidentiality" function it can be "used to keep communications secret." In its "identification" function it can be "used to provide forgery-proof digital identities." It enables freedom from regulation (as it enhances confidentiality), but it can also enable more efficient regulation (as it enhances identification).* (2006, p. 53)

In other words, cryptography can be used for confidentiality in favor of secrecy, as well as for authentication in order to validate identities. Digital signature authentication by means of cryptography guarantees the identity or authority of people operating in a digital environment such as Bitcoin, which is the digital corollary of establishing trust (Levy, 2001 p. 103. Once again, contrary to what Nakamoto promises, trust is not removed but instead established via a different mechanism. For this reason, Bitcoin affords pseudonymity rather than anonymity, meaning that users of Bitcoin are identifiable but not through a government-supplied ID [29].

In his history of cryptography, Levy reports that already in the 1970s it was foreseen that the advent of digital communications made cryptography essential, because computers and networks would make it possible to "…fully automate spying." (2001, p. 40). As the sub-title of his book suggests, Levy pits

[29] It is important to note that if one requires untraceability with Bitcoin, this is possible by 1. using anonymizing software such as Tor when using Bitcoin, and; 2. Creating a new Bitcoin address for each transaction.

American government that wanted to control and suppress cryptography, against libertarians who aspire to widely distribute the technology in order to protect civil liberties. Government wants to suppress and control cryptography in the name of national security, while libertarians argued that cryptography should be widely available in order to guarantee what cryptographers take as prerequisites for an open society, namely individual privacy and free speech[30]. Levy's book accounts of a tug of war between parties trying to suppress and distribute cryptography. From its inception cryptography in the digital sphere has been intertwined with politics and control. Furthermore, the cypherpunks applied cryptography to the concept of money in order to achieve financial privacy. Hughes argues that: "…privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system." (1993).

In the early 1990s cryptographer David Chaum established the company DigiCash in the Netherlands (Wallace, 2011). DigiCash launched Ecash, an anonymous electronic cash system that unlike Bitcoin did work with banks. DigiCash went bankrupt in 1998 and "…every effort to create virtual cash had floundered." (Wallace, 2011). Bitcoin thus far is the exception. Bitcoin is the latest effort in cryptography to introduce money that is put forward as "…convenient and untraceable, liberated from the oversight of governments and banks…" (Wallace, 2011). Wallace's statement of Bitcoin-as-liberator, Nakamoto's arguments expressed in the whitepaper and the political history of cryptography indicate that Bitcoin has a political nature[31]. Cypherpunk Timothy May argues that "Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions." (Peck, 2012). Wei Dai, who in 1998 created cryptographic *b-money*, argues that "My motivation for b-money was to enable online economies that are purely voluntary … ones that couldn't be taxed or regulated through the threat of force." (Peck, 2012).

When Nakamoto's paper that introduced Bitcoin came out in 2008, this was a time of financial unrest where Nakamoto's critical statements concerning the ability of governments and banks to manage the

[30] Hughes writes that ""…the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all." (1993).
[31] In a conversation on the Cryptography Mailing List, Nakamoto stated about Bitcoin that "It's very attractive to the libertarian viewpoint if we can explain it properly. I'm better with code than with words though." (2008).

economy fell on fertile soil. Bitcoin is put forward as the 'liberator' of the people suppressed by these powers, providing relief from having to trust bankers and politicians who arguably wreck the economy and rob the public of their wealth (Wallace, 2011). Bitcoin aligns with the political philosophy of libertarianism, which emphasizes freedom, private property, individual liberty and voluntary association. It puts forward "…the moral view that agents initially fully own themselves and have certain moral powers to acquire property rights in external things." (Stanford Encyclopedia of Philosophy, 2012) [32].

Libertarians are critical of states in general, where they argue that "…many of the powers of the modern welfare state are morally illegitimate." (Stanford Encyclopedia of Philosophy, 2012)[33]. Libertarians are of the opinion that no person has the right to coerce by means of force and that in this regard the state should not have any more power. Dai's statement cited earlier clearly expresses this sentiment with regard to voluntary association without the threat of force[34]. Bitcoin aligns well with this critical stance to government as mass adoption of Bitcoin poses a challenge to the current method of governments in generating revenues through taxation[35]. Furthermore, libertarians stress the importance of private property. Since Bitcoin are digital information in the form of ciphertext, Bitcoin is an implicit argument that digital information can and should be regarded as private property. Libertarianism is not confined to Bitcoin but more widespread in digital culture.

[32] The *Stanford Encyclopedia of Philosophy* states that within libertarianism a distinction can be made between right- and left-libertarianism, which depends on how natural resources can be owned.
[33] Depending on which sub-group within libertarianism one discusses, libertarianism wants a minimal nightwatchman-state, or no government at all.
[34] In 1992, cypherpunk mistrust of government and the use of cryptography combined with the idea of liberating money culminated with Jim Bell's publication of *Assassination Politics*. Debating libertarianism's principle of non-aggression, this articles argues that citizens should retaliate against misbehavior of government officials, lashing back at government coercion. It proposed an assassination 'prediction' market in which disgruntled citizens could punish violating politicians, pooling anonymous digital tokens that would be collected by the person who correctly predicted, but not necessarily caused, the death of the violator (Bell, 1992).
[35] From past experience with the combination of contemporary copyright, p2p software such as BitTorrent and the recording industry's business models we know that the Internet can have a disruptive effect on established organizations and their business models based on control of distribution. This observation has led Jon Matonis, who on his blog *The Monetary Future* describes himself as "…an e-Money specialist and crypto economist…", to state that "Digital cash is to legal tender as BitTorrents are to copyrights" (2012).

In their book *Who Controls the Internet? Illusions of a Borderless World*, law professors Goldsmith and Wu identify John Perry Barlow as perhaps the most famous poster child of cyber-libertarianism[36]. Barlow is the author of the 1990's manifesto *A Declaration of the Independence of Cyberspace*, in which he advocated a borderless Internet as a separate legal 'place' above and beyond government control (Barlow, 1996)[37]. Barlow is co-founder and vice-chairman of Electronic Frontier Organization (EFF), a highly visible organization build on libertarian ideals. The EFF was an early adopter of Bitcoin as the organization started to accept donations in Bitcoin[38] [39] [40]. In contrast to Chaum's E-cash and the online payments system PayPal that is built on top of existing banking infrastructures, Bitcoin does not relate to this infrastructure[41]. Its distributed design makes it not impossible but rather hard for government to regulate Bitcoin [42] [43] [44]. Furthermore, it enables Bitcoin to function as the payment system in cyberspace. Bitcoin resonates with the 1990s cyber-libertarian view of the Internet as a

[36] As the subtitle *Illusions of a Borderless World* shows, Goldsmith and Wu argue against Barlow's 'place' metaphor as well as against the notion that governments cannot touch the Internet.
[37] Interestingly in the context of this text, these authors here also identify Julian Dibbell as a libertarian, Dibbell being the author of the book *Play Money* whom I cited earlier in this text, which inquires into the apparent mix of play and labor in virtual worlds, as users create, buy and sell digital items
[38] [38] In the 1990s the EFF was also involved in cryptography, as it produced the controversial *DES cracker*, nicknamed *Deep Crack*, which was designed to demonstrate the insecurity of *DES*, the cryptographic standard adopted as standard by the US government.
[39] In the process providing the Bitcoin project with increased legitimacy.
[40] The adoption of Bitcoin by the EFF is also surprising when we look at an article from the 00's, in which Barlow argues that there should be no property in cyberspace. In the article *The Next Economy of Ideas*, Barlow writes about Napster and copyright, where he states that "The future will win; there will be no property in cyberspace." (Barlow, 2000).
[41] Interestingly, co-founder of PayPal Peter Thiel is a libertarian who originally had a similar liberatory vision for PayPal, where it would "…give citizens worldwide more direct control over their currencies than they ever had before. It will be nearly impossible for corrupt governments to steal wealth from their people through their old means because if they try the people will switch to dollars or Pounds or Yen, in effect dumping the worthless local currency for something more secure." (Jackson, 2004 p. 321).
[42] In a way similar to BitTorrent, Bitcoin does not directly link to a single discrete geographically-bound jurisdiction, but rather involves many legal systems and jurisdictions, making legal efforts not impossible but in practice rather cumbersome, costly and therefore impractical.
[43] I intent this example as a practical illustration and not as technical legality, given that elsewhere in this paper I argue that all software is 'in-material', indicating that it is by definition held in a physical container somewhere on Earth where a jurisdiction of a territorial government will apply.
[44] For this research I have engaged in an email conversation with one of the lead developers of Bitcoin, Wladimir J. Van Der Laan (VdL). VdL indicated that a government can opt to censor Bitcoin by means of 1. Getting local ISPs to block www.bitcoin.org, 2. Filter Bitcoin traffic, for example by means of deep packet inspection (DPI) by ISPs 3. Design a national Internet, such as Iran and North-Korea have done. Furthermore, any entity could sabotage Bitcoin by means of the 51% attack, exploiting Bitcoin's rule of one-CPU-one-vote. VdL deems this unlikely, given the high costs related to electricity and hardware needed for such an operation. At last, VdL explains that governments can reduce the credibility of Bitcoin by hiring 'experts' and have them argue through large media outlets, which he argues are in many countries controlled by a handful of corporations and families, that the contemporary centralized banking system is much better than Bitcoin.

separate 'place', which places a bounded Internet outside the control of the governments, supposedly far from the reach of the long arm of the Earthly laws.

Now I have introduced Bitcoin and its political nature, in the next paragraph I will go into Bitcoin's 'virtual' aspect. The name 'Bit*coin*' refers to cash tokens like coins and banknotes. Furthermore, Nakamoto and Wallace respectively define Bitcoin as 'virtual *cash*'. What does it imply that Bitcoin is called 'virtual'? In the next section I will discuss the politicalness of software and I will argue that the use of the term 'virtual' obscures the political nature of Bitcoin. I will illustrate this by introducing experts on the economies of virtual worlds. In a way similar to how Nakomoto argues that Bitcoin is an electronic analog of cash, these experts argue that 'gold' in virtual worlds functions exactly like cash in the 'real' world.

4. Politics of the 'virtual'

Nakamoto and others often do not explain why they chose to describe Bitcoin by means of the term 'virtual', or what this term signifies in relation to Bitcoin[45]. The term 'virtual' has a long history, originating from Medieval Latin *virtuālis,* meaning "influencing by physical virtues or capabilities" (Dictionary, 2012)[46]. In contemporary everyday language 'virtual' is used to signify *almost*, for example in response to the question "are you finished writing your thesis?" one might reply "Yes, virtually" meaning that you are almost, as good as but not really, finished. Furthermore, it has become customary to refer to phenomena related to digital culture by means of 'virtual', for example when we refer to Second Life and World of Warcraft as '*virtual* worlds'. On Wikipedia there is a list of over thirty things described as virtual, from virtual airline to virtual work (2012). On this wiki it is stated that ""…things are often described as "virtual" when *they share important functional aspects with other things* (real or imagined) that are or would be described as "more real"" (2012 emphasis mine).

[45] Bitcoin is not the only contemporary Internet phenomenon that is supposed to be an analogy of 'cash' on the Internet. In Sony's virtual world *Free Realms* users can buy memberships by means of a virtual currency called *Sony Station Cash*, which has to be paid for with what Lastowka interestingly describes as "real cash" (2010, p. 56).

[46] For example, in the fifteenth century there arose a debate concerning virtuality in which people literally lost their heads. Here, Catholics and Protestants argued about what happened when people took Holy Communion in the Christian Church. When eating bread and drinking wine, did they actually consume the body of Christ or did they do this 'virtually', i.e. in a symbolical way by means of their belief?

The differing uses of the 'virtual' above suggest it is applied in many field with differing connotations and denotations. The virtual is often positioned as opposing another term such as the material, the tangible or the real. In their book *New Media: A Critical Introduction* Lister et al. argue that the virtual as a philosophical concept is not the opposite of the real but a kind of reality itself. (Lister et al., 2009 p. 124). Lister et al. argue that we can no longer use the term virtual as an opposite of the 'real'. By adding the two terms together, virtual reality, we get differentiations within reality, rather than contrasts with reality (2009 p. 389). These differentiations are based on a reference to time. Consider again the everyday use of the virtual, the sense that a 'virtually' completed task is 'almost completed'. Completion is upon us, but not yet right now; it is not actual. Gilles Deleuze, philosopher of the virtual, maintains that the virtual is real, but inactual. Thus, the virtual exists, but not in the same way as things that actually surround us. Everything virtual is real, in Deleuze's Realist formulation of virtual realism: 'the virtual is not opposed to the real, but to the actual' ([1968] 1994, p. 208).

Being virtual is neither illusory nor unreal, it is a state produced by actual and material technologies; it can engage our physical senses and it can have real world consequences (Lister et al., 2009 p. 125). Bitcoin is actual software and thus has real world consequences. I want to stress this as software in general is often perceived as immaterial, due to its resemblance to language and its seemingly fleeting nature. This is what Schaefer, researcher in the field of digital culture, describes as "haptic inconceivability" (2011 p. 64). In other words, software seems ephemeral and it resists touch, i.e. it is intangible. However, Schaefer argues that software is always "'…in-material'; it is not only embedded in data carriers, it also must be perceived in terms of materiality, because it creates means of production." (2011 p. 64). Following this statement, software is something which may resist immediate physical contact, "…yet which is incorporated in materiality rather than floating as a metaphysical substance in virtual space' (Van den Boomen et al. 2009 p. 9). Schaefer concludes that "The in-materiality of software emphasizes that symbolic language, action – meaning actual performance – and socio-political issues of the material world are inextricably linked (2011 p. 64).

It becomes clear that in popular culture the term virtual is used in a different way compared to its philosophical definition. This makes the philosophical discussion of the virtual irrelevant compared to the virtual as applied to Bitcoin. Neither Nakamoto nor commentators such as Wallace, who use the

term 'virtual' to describe Bitcoin as virtual cash, refer to Deleuze and the philosophical virtual. By using the term virtual, Nakamoto and others have the more modest intent of communicating that Bitcoin is in some respects is like cash. In a way similar to how Szabo explains that with *bit gold* he tried to mimic certain characteristics of gold, Bitcoin is designed to be an intangible model of cash working over the Internet. Furthermore, the virtual in relation of Bitcoin communicates that it is a phenomenon related to digital culture, to computing and the Internet; Bitcoin is software that is said to share some functional aspects with something else, here cash. Besides cash, Bitcoin is also said to be in some ways like gold, where Nakomoto draws analogies between Bitcoin verification and gold mining.

In the context of Bitcoin's analogies of 'mining' and 'farming', it is relevant to consider the similar practice of 'gold-farming' present in digital culture, namely in World of Warcraft (WoW) and other Massive Multiplayer Online Role Playing Games (MMORPG's) and virtual worlds. Here, users who are predominantly located in lower-wage countries such as China perform long hours of sweatshop-like labor collecting 'gold', the currency of WoW with which in-game items can be bought. Instead of the 'mining' metaphor in case of Bitcoin, this practice is referred to as 'farming', analogous to agricultural practice. WoW gold is exchanged for currencies such as the euro and dollar in a process popularly called *Real-Money Trading* (RMT)[47]. Bitcoins can be exchanged for currencies via online exchanges such as MtGox. In addition, both Bitcoin mining and goldfarming practices are enabled and regulated through code; gold farmers can only acquire as much gold as the protocol affords and Bitcoin miners only as much Bitcoins following the principles described earlier[48] [49].

In his book *Play Money,* journalist Julian Dibbell describes his research after gold farming in virtual worlds and his own experience as a gold farmer (2006). Here, he states that people are able to earn an

[47] The recently released game *Diablo III* is the first mainstream game to include a managed, in-game 'Real Money Auction House' (RMAH). Here, players can exchange what the designer and owner of this game, the limited-liability corporation *Blizzard Entertainment,* describes as 'virtual objects' for 'real', 'actual' money via the online payments service PayPal (Diablo III Auction House FAQ, 2012).

[48] A crucial difference between them is that with Bitcoin the total amount of currency existing in the economy is transparent through its code, rising at a predictable rate over time, up to a pre-defined maximum as explained earlier. In contrast, the amount of gold outstanding is unknown by users of WoW; it is a black-box and also potentially unlimited. In other words, there is no pre-defined maximum and for users the rate of creation is an unknown variable.

[49] Another difference is that Bitcoin is more like the 'macro's, or exploits, that were pieces of additional code for virtual worlds, designed to let the game characters automatically undertake actions in the game, such as collecting gold or loot. With these pieces of code in place, the process could be left running unattended, instead of requiring manual labor. In principle, once the Bitcoin setup is in place and running, it does not require such human attendance.

income in virtual worlds, a small group reportedly earning so much that they no longer have a typical day job in the so-called 'real' world. Dibbell's key argument is that when the economy 'in' virtual worlds such as WoW interacts with the economy of planet Earth through RMT, play becomes productive and "Production is melting into play" (Dibbell, 2006 p. 25). Dibbell calls this development 'ludo-capitalism', combining the terms capitalism and the Latin word 'ludus', meaning 'play'[50] [51]. Although the question whether Bitcoin is a playful phenomenon is outside the scope of this text, my point here is that the practice of goldfarming has been important in paving the way for Bitcoin 'mining'[52] [53]. What goldfarming demonstrated is that people are willing to invest in the creation ('farming') and acquisition, buying and selling of intangible digital objects, essentially digital information, implicitly regarding these as private property and treating them as assets[54] [55]. However, in stressing similarities we should not forget that Bitcoin might also in some respects differ from the modeled phenomenon.

[50] The coinciding of play and work is also known as ´playbor´, contracting play and labor (Heeks, 2010 p. 7).
[51] Buying and selling digital objects is in principle a surprising development, given that digital copies are what economist call ´non-rivalrous'. This follows the copy affordance of computers'. When one has a physical object under private property in real space and another person takes it, the person who loses it can no longer enjoy it. However, in cyberspace one does not take the object but makes a copy, which makes that both persons can enjoy it. The number of copies one can make is practically unlimited, limited only to the space of storage media such as harddisks where the cost per copy is in practice negligible.
[52] Bitcoin is obviously different from virtual worlds, for example in that most virtual worlds are owned by legal entities, often incorporated as for-profit limited liability corporations (LLC) that can be held accountable through law by the jurisdiction of their incorporation. Users of virtual worlds enter into contract with these legal entities through the 'click-wrap' EULAs, written in 'legalese' that most people in practice do not read. Alternatively, Bitcoin is non-profit open-source software with an MIT license, provided 'as-is' and as such goes without a legal entity, which makes it harder to regulate by law.
[53] Lastowka in his book *Virtual Justice* argues against Dibbell's ludo-capitalism by stating that the conceptual integration of play and labor is "morally dangerous, given that "…game rules, unlike the rules of law, do not even aspire to achieve social justice, much less prioritize those strategies that are efficient in doing so. A boundary can and should be identified between games and "ordinary life." Such a boundary is not only observable, but essential to the institution of government." (2010, p. 117)
[54] Virtual worlds could in principle simulate abundance without constraints modeled after planet Earth, but Dibbell notes that such superabundant worlds such as *Worlds Away* and *The Palace* have been tried and tested but it turned out that people did not like these worlds as much as those with constraints (2006 p. 41). This observation by Dibbell is also made by Castronova in his book *Synthetic Worlds* and by Lastowka in his book *Virtual Justice*. The code of virtual worlds is 'voluntarily' chosen to disable the copy affordance of the computer. Readers familiar with the film *The Matrix* (1999) will recognize in Dibbell's narrative the scene in which the character Agent Smith explains that the first Matrix was designed to be ´perfect´, but this 'perfect world' was rejected by humans who arguably define their reality through 'misery and suffering'.
[55] Lastowka also argues that it is debatable whether these laws *should* apply, given 1. the era in which these laws where crafted, 2. The fact that the Internet had not yet arrived in those times, and 3. That law responds to the arrival of new technologies such as the aircraft, in case these technologies pose a challenge to the way law reaches certain outcomes deemed desirable by society, i.e. justice (2010, p. 67-71)

Some of these differences are obvious; for example Bitcoin is intangible, unlike the tangible cash that it is supposed to model. Other differences between Bitcoin and cash are more subtle. Earlier, I explained that Bitcoins are created through its block chain protocol. Here, choices are made with regard to procedures, i.e. how Bitcoin 'works', and it is here that the political nature of software and thus of Bitcoin manifests itself[56]. Lawrence Lessig stresses the 'politicalness' of software design as he argues that "code is law"[57]:

> *In real space, we recognize how laws regulate—through constitutions, statutes, and other legal codes. In cyberspace we must understand how a different "code" regulates—how the software and hardware (i.e., the "code" of cyberspace) that make cyberspace what it is also regulate cyberspace as it is.* (2006, p. 20)

Lessig continues by arguing that code "…determines what people can and cannot do." (2006, p. 77). Lessig states that when we look at competing values and choose among them, we call these choices "political" (2006, p. 78). Decisions like these are about how the world is ordered and which values are awarded precedence. Choosing among values, making decisions about regulation and control, "…all this is the stuff of politics." (Lessig, 2006 p. 78)[58] [59]. Lessig illustrates this by means of an example I have introduced earlier in this text, namely Massive Multiplayer Online Games (MMOG's), where "…the possibilities in MMOG space are determined by the code—the software, or architecture, that makes the MMOG space what it is" (2006, p. 14)[60]. Software architecture programs values in code[61].

[56] As an example, it is illustrative to note an argument on the wiki of *Bitcoin.it* I referred to earlier. Here, it is stated that "The creation of coins must be limited for the currency to have any value." (2012). These authors on *Bitcoin.it* here adhere to the classic economic dictum associated with neoliberalism, namely that the 'invisible' hand of supply and demand, i.e. the market, is at work. This argument was brought forward by Adam Smith, founder of the *political economy* philosophy. This statement on the Bitcoin.it website is an argument that builds on a certain worldview with its associated values and politics. Although Bitcoin attempts to be an alternative to contemporary cash, these authors cannot escape what Rushkoff in his book *Monopoly Moneys* calls the "market dogma" (2012, p. 253).

[57] Lessig did not intend 'code is law' as an equation, but rather like an analogy, indicating that in cyberspace code functions *like* the law we are more familiar with.

[58] In the context of the political nature of money, Graeber argues that "Politics, after all, is the art of persuasion; the political is that dimension of social life in which things really do become true if enough people believe them." (2011, p. 342)

[59] Rushkoff states that contemporary money is naturalized as the only possible to which no alternatives have existed or can be thought to exist (2012, p. 197)

[60] In addition, following the argument in chapter *2.1 The distributed block chain,* in MMOG 'space' the possibilities are not only determined by code, but in addition the 'space' itself also consists of code.

[61] Given that these 'spaces' increasingly form the environment in which people live, highlights the political power of those

In his book *Synthetic Worlds,* Castronova, an expert on virtual world economies, argues in line with Lessig that the code of MMOG's determines what is and what is not possible. Castronova validates that a programmer, which he refers to as the 'coding authority', make choices with regard that code will and will not permit. Castronova writes the following about the endowment of diamonds in virtual worlds and the 'real' world:

> *On Earth, these items tend to be quite expensive. … Their beauty contributes to their price, of course, but so does their scarcity. Now, what if the Earth could be induced to produce as many diamonds as anyone would ever want? Such a thing is impossible here, but not in cyberspace. The coding authority who owns and controls a synthetic world could pave the streets with diamonds if it desired. .... All of these coding decisions would affect the price of diamonds and the happiness of the people wearing them. … our planet is endowed with a certain availability of diamonds based on their presence in the ground and our understanding of how to get them out of the ground. In synthetic worlds, things are different. The availability of diamonds is not an endowment but a choice. Thus while the mental objects in play there (beauty, price, love, profit, scarcity, reputation, power) are nothing new, the rulebook under which they are all contested is a new thing indeed.* (2005, p. 8 emphasis mine):

Castronova argues that on Earth constraints are pre-determined by nature. This is the notion of scarcity as put forward by the field of economics, the academic discipline that studies how people make choices under this condition of scarcity. In contrast, Bitcoin's endowment is the result of many choices made by its programmers between possible alternatives. For example, Bitcoins are 'artificially' scarce[62] [63].

able to read, edit and write code.

[62] I have borrowed this term from Lastowka, who in his book *Virtual Justice* puts forward an argument similar to Castronova's diamond narrative (2010, p. 135-136). An interesting question that demands attention is whether scarcity in relation to the supposedly 'real' world, planet Earth, is not also 'artificial'. Artificial here meaning a concept that is put in place by *humans*, not nature, through private property rights, given that these rights are what "…structures interpersonal relations concerning things…". (2010, p. 130). Lastowka suggests that this law is more about the relations between people, rather than between people and things. So, we might ask; is scarcity an endowment of nature or does it result from this man-made law?

[63] Lastowka also notes that many Earth-bound commodities, such as *diamonds*, "…are produced in *intentionally limited*

Through code this arbitrary voluntary constraint becomes an endowment for users who accept the system[64] [65]. Given that money occupies an important position within economics, Castronova also endeavors to explain what gives value to money in the 'real' world. Furthermore, he argues that this works in a similar way in virtual worlds. Castronova makes the following statement about 'gold', the money of virtual worlds such as WoW:

> *It is frankly impossible to deny that the gold pieces of fantasy worlds are money, just like the money in your pocket. They are sustained by exactly the same social mechanisms and perform exactly the same functions.* (2005, p. 151 emphasis mine)

It is important to note that Castronova does not refer to the more general 'money' or 'currency', but to the tangible money tokens, the 'hard' cash in your pocket. In addition, in a way similar to how Nakamoto explains Bitcoin, Castronova asserts that the gold pieces in WoW perform *exactly* the same functions as cash is supposed to do in the 'real' world, arguably sustained by the same "social mechanisms". Paradoxically, Castronova in his text also states that the objective of the designers of virtual worlds is not virtual reality, but "selective fidelity", which means that "The simulation had to render only the things that mattered for the exercise in question." (2005, p. 88). In other words, for the world to be believable it has to simulate some observable qualities demonstrating functional likeness; gold in WoW is money because it performs the same function as cash. However, Castronova also puts forward that the copy, the simulation, does not in any way need to be complete or perfect. In other words, it is not *exactly* the same. This is understandable, as there is no point in arguing that e-mail is *exactly* the same as snail mail, or that the soccer simulation game *FIFA 12* is identical to the sport of

quantities with the understanding that limiting supply increases demand. In some cases, a higher price signals the prestige value of a "luxury" or "limited edition" artifact. Goods whose high price drives demand are known as Veblen goods. Yet the legal system, when it fixes the value of good, does not discount the legal value of Veblen goods. When a *diamond* or luxury sedan is stolen, the law values that object at a market price that compensates owners for losses attributable to regimes of privately imposed scarcity." (2010, p. 137 emphasis mine).

[64] It is important to note that this observation also holds for contemporary money, given that monetary policy determined by central bank forms the basis for the endowment of money.

[65] A question that is worth asking is why the cap on the number of Bitcoins was set at 21 million and not more or less; what makes 21 million 'right'? Nakamoto does not justify this number in any way. After asking this question on Quora.com, I got the following answer from Ron Gross, a self-identified "Bitcoin evangelist and believer", indicating that this number is rather random: "Arbitrary number that "just felt right" to Satoshi." (2012)

soccer that it purports to model[66]? Furthermore, in case of Bitcoin we should not expect perfect exactitude, given that Nakamoto is critical of certain aspects of the system that he models. In other words, if Bitcoin would be a perfect copy nothing would be different, resulting in more of the same. This is not why Nakamoto developed Bitcoin. On the contrary, political change is the motivation and Bitcoin is the argument. Bitcoin is a prime example of Schaefer's argument that software is intertwined with the politics of the material world.

Castronova uses circular logic to assert that no model is perfect; only what matters for the exercise in question, matters for the simulation. This means that the coding authority has determined what matters. In other words, programmers have decided what behavior the software should allow and what is will constrain. Therefore, I suggest that; 1. we should ask "*who decides* what 'matters'?", and; 2. Determining what matters is a question of a political nature that determines which values are awarded precedence as these are embedded in code. In his book *Play Money,* the libertarian journalist Julian Dibbell disposes of questions such as these, which he calls unnecessary and time-wasting 'ontological' questions. Dibbell agrees with Castro nova that[67]:

> *"…whether its conversational intelligence or rush-hour traffic or nuclear reactions you're seeing modeled in digital form, it is always just that: a model. And that therefore "it's a waste of precious time and creativity to wonder whether the model is the same, on some deep, ontological level as what it simulates. The question, rather, is whether it's the same in every way that matters for the purposes at hand."* (Dibbell, 2006 p. 108 emphasis original)

[66] In case someone argues that *FIFA 12* is somehow the best model of soccer, this is relatively innocent since one can easily switch to a marketed alternative such as *Pro Evolution Soccer (PES)*. However, when the argument concerns money, I argue that a similar argument is more problematic, given that money is a standard shared by most participants in society at large. The economist Robert Guttmann in his book *Cybercash* stresses the importance of money by highlighting this 'public' nature: "…money serves as a *public good* inasmuch as its proper functioning – in terms of the modalities of its creation, its smooth circulation and its stable valuation – yields such large social benefits that you would not want anyone to be deprived of those." (2003 p. 23).

[67] In their book *Who Controls the Internet?*, law professors Goldsmith and Wu identify John P. Barlow as (cyber)libertarian, while according to them Dibbell shared with Barlow the powerful libertarian vision of the Internet as "…a new frontier, where people lived in peace, under their own rules, liberated from the constraints of an oppressive society and free from government meddling." (2006 p. 13). The reader will recognize in this narrative the words of Nakamoto who describes Bitcoin as a 'liberator', which I cited earlier in the chapter *Introduction to Bitcoin.*

I do not consider it problematic that Bitcoin is modeled after cash, or said to be modeled after cash. This is understandable from the point of view of those who present it, given that by suggestively naming the model and referring to other phenomena Bitcoin is awarded a location linked to other concepts in people's mental frameworks. This practice is not an isolated case, but more prevalent in digital culture, where the Graphical User Interface (GUI) introduced in the 1980s is a prime example. The GUI allowed users to interact with a computer through images rather than text where the software modeled aspects through a desktop metaphor in which the display models a desktop, upon which documents can be placed[68] [69]. Since the advent of Internet, people have struggled to understand Internet phenomena and many metaphors and analogies have been applied to figurally 'grasp' the abstractness of the Internet. Barlow's analogy of the Internet as a separate 'space' I mentioned earlier is one of these analogies. Bitcoin is no exception as it is explicitly put forward as a model of cash[70].

The key insight here is neither the practice of modeling nor the application of metaphors or analogies, but rather that in stressing the similarities of the 'model' to that which it is modeled after, the differences remain undiscussed. Furthermore, this may cloud the fact that models are not copies of a 'perfect' exactitude. There might be important differences that exist side-by-side the properties that are put forward as functionally equivalent, which make that the replica overall does *not* function in exactly the same way. By definition a model is presented as a simplified, reductive representation of (a part of) reality. Hence, inherent to a model is that not all properties or dimensions are included. In other words, Bitcoins and 'gold' in virtual worlds are probably in many ways *not* like the money in your pocket. In addition, models are not neutral, but *contested*, or at least contestable. Therefore, I strongly disagree with Dibbell's down-playing position on what he refers to as the 'deep ontology' of the model. Dibbell and Castronova argue that only those things matter, that matter for the purpose at hand. However, what 'matters' is not pre-given but determined by an 'authority' in a political decision-making process.

[68] This presumably made it easier for non-programmers to interact with the machine, contributing to the widespread success of the personal computer, given that it was no longer necessary for such a user to familiarize his- or herself with the more technical details of the machine before completing a relatively simple task, such as typing a letter. One might compare this with the driver of a car, that does not have to be familiar with the workings of the machinery 'under the hood' such as the internal combustion engine, in order to drive the car.
[69] More examples are chat*rooms*, virtual *worlds*, the web 'page' and MS Word's 'document' that refers to paper.
[70] As well as gold (Nakamoto, 2008).

Dibbell continues his argument by stating that as we move along in cyberspace over time, producing more and 'better' models, we should uncritically adopt them at face value:

> *"…As the universal machine continues to replicate more and more of the real world's subsystems, with more and more of the real world's compelling subtlety, it will surely just get easier to fall into the habit of accepting our digital "other worlds" and "second lifes" as functional equivalents of the originals."* (Dibbell, 2006 p. 110 emphasis mine)

According to Dibbell, the replica's model (sub)systems and over time these models will somehow get 'better'[71], which should make it easier to 'fall into the habit' of accepting these replica's as functionally like the original; we should accept, not contest. I disagree and suggest that succumbing to Dibbell's 'habit' is more like falling into a trap, falling for what those who program code deem important enough to define in code. In effect, they would be deciding on 'what matters', while obscuring what is probably more important; namely that what supposedly does not matter, and shoving what is left out of the model under the veil of the 'virtual'. We should contest the 'ontology' of the politically loaded model, debate what we deem important enough to include and what not. In case we follow Dibbell in 'accepting the habit' without analyzing beyond face value, without asking what is different, we might unknowingly award certain values precedence over others. Bitcoin's discontinuities have to be demystified further than the 'virtual', uncritically accepting the self-referential logic of the fallacy 'what matters, matters' and the judgment of those who get to decide on this matter.

I do follow Castronova when he states that "…the term *virtual* is losing its meaning. Perhaps it never had meaning." (2005, p. 148). In this context, the lawyer of Linden Lab, has put forward a simple but relevant remark[72]. In the context of a lawsuit brought against the company by a user concerning the removal of his account including 'virtual assets', lawyer Yoon stated that the 'virtual land' in Second Life was not 'real' land: "The term 'virtual' may not have a strict legal interpretation, but if anything it means that the thing being described is NOT what ever comes after the word 'virtual.'" (Yoon in Lastowka, 2010 p. 17). Since Bitcoin is positioned relative to cash, it is also important to review what

[71] More 'real', perhaps? In a way similar to how the *FIFA* soccer simulation games are getting 'more realistic' every consecutive year?
[72] Linden Lab is the corporate owner of the virtual world Second Life.

contemporary cash is, in order to note important differences between cash and Bitcoin. Related to this is the question why Bitcoin commentators refer to cash and not the more general 'money' or 'currency'. I will first introduce the contemporary money system, which will include a brief analysis of the fractional-reserve banking practice and the concept of debt. Hereafter, I will discuss the status of cash in this system, which will include a discussion of the (in)tangibility of both money and cash.

5. Contemporary money system

The contemporary money system is organized by central and commercial banks, managed through the principles of accounting and the fractional-reserve banking practice[73]. Money is created as debt through loans and transactions are managed via this system. Here, government-sanctioned private institutions called central banks have a monopoly on money. Via monetary policy, the central banks determines the volume of what is known as 'base money', often through loans to the government[74]. In the contemporary money system, money is created as debt, administered by banks. This has led Bernard Lietaer, the former President of Belgium's Electronic Payment System and implementer of the convergence mechanism (ECU) to the single European currency system, to state in his book *The Future of Money* that "Money is modern society's central information system (2001, p. 22).

[73] Here I refer to the European system and the Euro (€).
[74] In the Netherlands, *De Nederlandsche Bank N.V.* (the Dutch National Bank) is a private corporation in which the Dutch government, via its department of Treasury, is the only shareholder. The European Central Bank in turn resembles a corporation, where the member national banks are its shareholders. The ECB has legal personality under public international law.

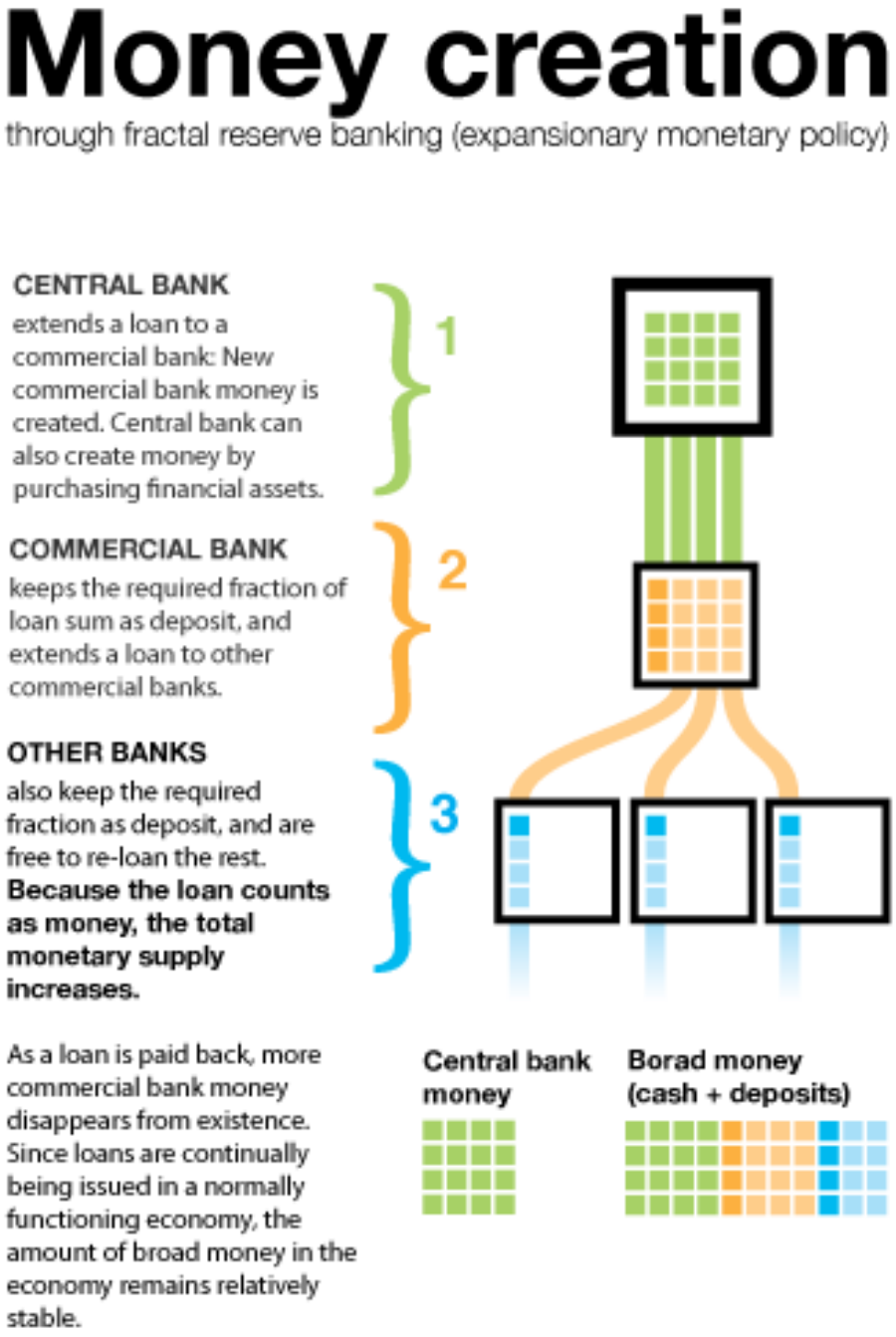


Figure 4. Money creation via the fractional reserve banking practice. Note: 'borad money' is a typo, which should be 'broad money'. Source: http://upload.wikimedia.org/wikipedia/commons/f/f2/Money-creation.gif

After central banks have created 'base money', commercial banks are also allowed to create money by means of the so-called 'money multiplier' enacted by the fractional reserve ratio imposed by the central bank[75]. This means that commercial banks maintain money reserves that are a fraction of its customer's deposits. The fraction is called the reserve ratio, which is the percentage of deposits that the bank keeps as reserve. For every deposit of money at the bank, the bank keeps a percentage as reserve and may loan out the rest of the amount. Here it is important to note that, contrary to popular belief the bank does not only loan out money that is deposited by its customers. In addition, a new extra amount is issued, thus the commercial banks in effect issue new money (see Figure 5). Some of the money that is loaned may subsequently be deposited again with another bank, repeating the process of increasing deposits at that second bank and all[76]owing further lending[77]. The fractional reserve banking practice increases the money supply, and banks are said to create money.

Due to fractional reserve banking, the broad money supply of most countries is a multiple larger than the amount of base money created by the country's central bank. Nakamoto is critical of this practice that (s)he holds responsible for banks lending in "…waves of credit bubbles *with barely a fraction in reserve*. (2008, p. 1 emphasis mine). The Bitcoin report by the FBI validates that "…central banks can *arbitrarily* increase the supply of currency…" (FBI, 2012 emphasis mine). Bitcoin retains the paradigm of scarcity inherent to contemporary monetary policy, as it limits the supply of Bitcoin tokens like the central bank limits money volume. However, Bitcoin desires to make the black-boxed discretionary actions by central bankers more transparent, as the progression in volume of Bitcoins over time is an outcome of its code which is open to public scrutiny (Grinberg, 2011 p. 168). I have shown earlier that Bitcoins are created through a different mechanism than debt. In order to further identify the similarities and differences of Bitcoin to cash, it is necessary to delve further into the history of debt, which has implications concerning the tangibility of money and cash. In turn, it will explain why

[75] The money multiplier is determined by the reserve requirement. For the sake of completeness it is worth noting that although the central bank monetary sets an upper bound of money volume, the actual broad money supply is also influenced by other variables, such as whether commercial banks keep reserves 'in excess' of the requirement. In addition, it is also dependent on whether the money that is lent out is deposited with a bank again after the loan has been made, or kept as *cash*. Thus, fractional-reserve banking does not apply to cash not deposited at banks, but held in possession by non-bank businesses or consumers.
[76] As noted earlier, the volume of Bitcoins is also arbitrary.
[77] Here, the process is again identical as described herefore, where the bank keeps a fraction of this amount as reserve and issues new money by the amount that remains.

Bitcoin is put forward as a model of cash.

In his book called *Debt: The First 5.000 Years,* David Graeber, an anthropologist who had an early role in Occupy Wall Street in 2011, reviews the history and moral implications of debt[78]. Contrary to popular belief, Graeber argues that money is not a tangible object, but an intangible 'imaginary' standard. Graeber's puts forwards the revisionist argument that money did *not* spontaneously emerge to address a social necessity. Graeber argues against the notion that the *raison d'etre* of money is the suggested inefficiency of barter in facilitating humanity's 'natural' tendency to trade, as economists have argued since Adam Smith (2011, p. 25). Graeber disagrees as he argues that Smith's story, the story of barter and the social need for a third commodity that everybody stockpiles as currency, is "…the great founding myth of the discipline of economics." (2011, p. 25). Graeber emphasizes that due to this naturalized narrative central to the discourse of economics, many people hold the erroneous belief that people naturally want to trade, thus a medium of exchange was just waiting to happen. Graeber states that anthropology has found no evidence that this ever took place and much evidence that it did not (2011, p. 28-29).

In the story of barter the problem of the 'double coincidence of wants' was prevalent[79]. Since money such as we know it today was not yet invented, how did people solve this problem? Graeber argues that the problem of the 'double coincidence of wants' simply does not exist in the hypothetical scenario where two people in a small community would 'exchange' commodities, because the 'buyer' might not have something the 'seller' wants right now, "But if the two are neighbors, it's obviously only a matter of time before he will." (Graeber, 2011 p. 36). In the context of this type of small village community, the givers and takers of the commodities have ongoing relations with each other. In case one provides someone else with something, the 'seller' registers an imaginary intangible credit and the 'buyer' a debit; he becomes indebted and 'owes him one'. This entails that contrary to Smith's argument there is

[78] Graeber in his book discusses the morality of debt, locating the concept in the religions Christianity and Islam. Graeber quotes parables from the Bible and points out that in many languages the word 'debt' is the same word as 'sin' (2011, p. 56). Graeber argues that debt has become the most profound moral obligation in our reality.
[79] This refers to the imaginary situation, where two people willing to trade would have at the same point in time need to have something of approximately the same value that the other person would be interested in.

no need for people to stockpile a commonly accepted commodity, a tangible medium of exchange. Instead, most transactions were based on credit, where no tangible object changed hands.

Money was not a medium of exchange in the sense of a tangible object one can hold and exchange. It did not 'change hands' [80]. Lietaer asserts that the belief that money is a tangible object is "…a key illusion in the magic about money" (2001, p. 46). Instead, money was a unit of account, a non-tangible standard, i.e. a 'numéraire' which is a basic accounting standard by which value is computed mathematically[81]. The system of debits and credit allows society to track resources and keep score in general. Now we accept money to be the yardstick that measures, what does it measure? In the contemporary money system it measures obligations, money is quantified debt that signals 'I owe you' (IOU) (Graeber, 2011 p. 46). Banks are awarded the privileged position as 'guardians' of the debt relations between ordinary citizens, granted by law and ultimately enforced by government coercion[82]. As shown earlier, the libertarian cypherpunks are wary of this organization based on force in which they have no choice, feeling obliged to participate in a system to which no alternative is allowed to exist.

The narrative concerning monetary history offered by Graeber is important in relation to Bitcoin, since Bitcoins are not created as debt but via the verification process I described in the chapter *Introduction to Bitcoin*[83]. This configuration has profound implications concerning the functioning as well as the outcomes of Bitcoin, compared to how contemporary money 'works'. Media theorist Rushkoff puts it as follows: "Akin to the operating system of a computer, currency creates the rules by which its applications must play" (Rushkoff, 2012 p. 197). For example, one of the rules of the current system is that it is standard practice to apply (compound) interest on loans. Since money is created via loans, this entails that interest is a universal practice. Bitcoins are not created as debt and interest in principle does

[80] As a thought experiment, I invite those who hold the belief or have the desire that money is tangible, to compare this to other standards, such as the hour, the watt, the decibel or the cubic meter. Has one ever touched an hour? One can touch a shekel as much as one can touch an hour.
[81] Money is thus primarily is a way of comparing things mathematically, as proportions, such as six of X is the equivalent of 1 of Y (Graeber, 2011 p. 52). Things find a common denominator in money, which enables the comparison of apples and oranges.
[82] "…it is law that enforces contracts, establishes property, and regulates currency…" (Lessig, 2006 p. 127).
[83] Since contemporary money is quantified debt, debts can be denominated *in* Bitcoins, but Bitcoins are not created *as* debt.

not apply, at least it is not part of its protocol[84]. I mention interest here sideways, but to illustrate the drastic effects of Bitcoin omission of interest, I again refer to banker Lietaer who has noted three important consequences of the way interest is a default practice systematically build into the money system. These consequences are:

> *1. Interest indirectly encourages systematic competition among the participants in the system.*
> *2. Interest continually fuels the need for endless economic growth, even when actual standards of living remain stagnant.*
> *3. Interest concentrates wealth by taxing the vast majority in favor of a small minority.*
> (2001, p. 56)

In order to refrain from technological determinism, I suggest that the intricacies of Bitcoin and its user interactions remain to be inferred. However, if interest would only be a weak factor in the complex system that give rise to the consequences noted by Lietaer, we can expect that Bitcoin might result in different outcomes. Given that Bitcoin is specifically positioned as an electronic analog of cash, I will now go into the status of cash in the contemporary money system.

According to popular but wrong belief, money is printed or minted into existence as tangible cash. However, as argued before, money is an abstraction, 'created' as intangible numbers administrated by banks as debt. The central bank is the authority that *issues* money by typing numbers into an account as a credit and noting a corresponding debt, where the debtor promises to pay this principal amount, the IOU, back at a later time[85] [86]. These abstract numbers can be contained by paper as well as in an electronic medium[87]. For banks it is customary to distinguish between tangible and intangible money. The numbers held in a bank ledger are called giral money and tangible cash tokens fall in the category

[84] In a way similar to how the concept of debt can still be applied to loaned Bitcoins, interest can also be applied to a loan of Bitcoins. However, contrary to the contemporary organization, this is not a default feature of the system like it currently is applied, namely already at the source of money and onwards.
[85] Often including an additional sum called interest.
[86] Graeber in his book challenges the assumption that debts have to be repaid (2011p. 3).
[87] In a short analysis made of Bitcoin, Victor Grishchenko, a post-doctoral student of infocentric networks and deep hypertext, argues that "As the backend of the contemporary banking is definitely paperless, the real money is *already* e-money." (Victor Grishchenko, 2011)

of chartal money. The two categories of giral and chartal money are illustrated by Figure 6, which shows that the volume of chartal money has remained quite constant over time, while giral money has increased following fractional reserve banking practice. However, despite the distinction drawn between giral and chartal money, their common denominator is that both are liabilities accounted for on bank's balances[88].

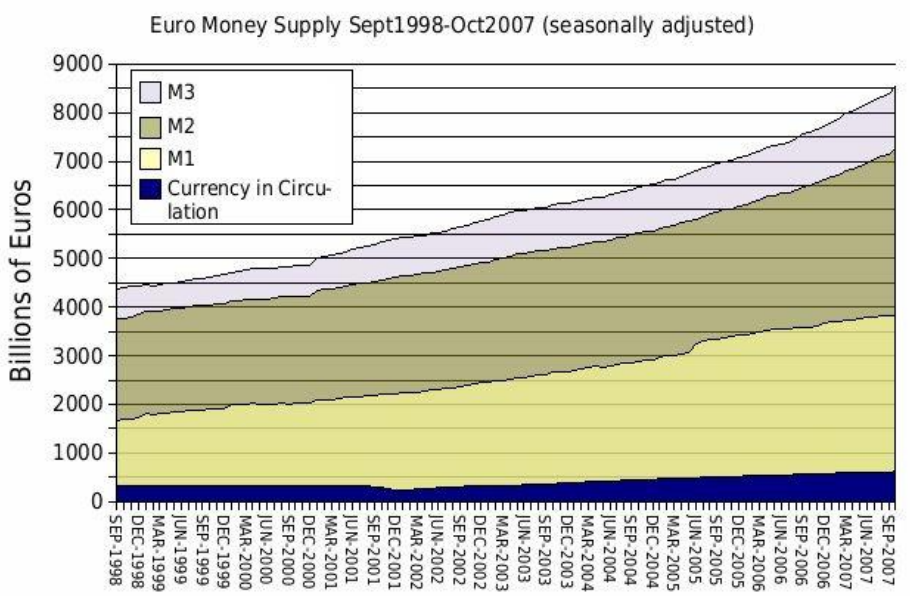


Figure 5. Volume of outstanding giral and chartal Euro's in 1998-2007. Source: http://upload.wikimedia.org/wikipedia/commons/d/d0/Euro_money_supply_Sept_1998_-_Oct_2007.jpg

Printing or minting paper or metal happens in concordance with the central banks who issue the debits and corresponding credits. The creation, printing or minting, of the tangible cash objects is dependent on the issuance of the debits and credits in the books. These banknotes and coins refer to debt and the

[88] In the context of Bitcoin, where Nakamoto lumps together banknotes and coins together in the category 'cash', it is worth mentioning that banknotes and coins are accounted for in separate ways by the European Central Bank (ECB). I have engaged in an email conversation with the ECB, from which I have understood the following. Banknotes in circulation are accounted for as a liability in the balance sheet of the ECB titled 'Banknotes in circulation'. In the euro area coins are treated differently than banknotes, for legal reasons. Not the central bank system, but the governments mint coins and bring them into circulation. The respective national central banks register a debt from the bank to the governments for the coins by giving the governments a claim (liability) on the central bank, which can be found under the liability item titled "Liabilities to other euro area residents/General government" (ECB Balance Sheet, 2012). However, what is similar between banknotes and coins is that also with coins, the ECB's Governing Council has to approve the volume of coin issuance for each government before they can mint the coins. The issuance of the intangible numbers 'in the books' is necessary for the minting of coins to occur.

notes and coins exist of proof that the holder, the bearer of the note or coin, has title to the debt. Cash is a standardized credential which provides authentication to a bank that the bearer of the note or coin has valid title to the credit administered by banks[89]. In other words, the 'you' proves title to the debt of 'I' in IOU. Thus, someone who pays with cash does authenticate, but not by means of a government I.D.; it is not required to supply personal details along with the token as it is transferred from person to person.

It is this credential aspect of cash that makes that cash can be falsified. Furthermore, this type of authentication is also what cryptographers acclaim, namely that it allows for privacy. It also explains why Bitcoin is positioned explicitly as a model of cash and not modeling the more general money or currency, i.e. the debt and credit relations between legal entities in the contemporary money system that are tied to identities[90]. In other words, intangible Bitcoin tokens in fact model the credential function of the tangible cash token media that functioned as proof of title to intangible money 'in the book's'. As argued earlier, Bitcoin tokens instead do not relate to debt but exist independently as privately owned information 'objects' in the network. To conclude, the goal of this analysis was not to disqualify Bitcoin as opposed to contemporary money, neither am I suggesting that Bitcoin is the definitive ideal money model. I suggest that Bitcoin's highest achievement might be that it, as a mere alternative available, provides insight into the structural biases of the contemporary money system (Rushkoff, 2012 p. 197). Bitcoin-as-alternative may assist in realizing a perceptual shift, as a new lens that helps us to see, to reveal the structural biases of an ancient naturalized medium that until now remained largely invisible as it quietly but consistently ran in the background[91].

6. Conclusion

I have introduced Bitcoin, the open-source software project based on cryptography and p2p technology that was launched in 2008. Bitcoin is the latest in a series of projects put forward by libertarian cryptographers, who argued that anonymous transaction systems were necessary for an open society.

[89] Chartal is derived from the Latin word 'charta', meaning token or ticket.
[90] Bitcoins are made tangible again, completing the cycle of abstraction by means of a metal Bitcoin token 'coin', which is "…a collectible coin backed by real Bitcoins embedded inside. Each piece has its own Bitcoin address and a redeemable "private key" on the inside, underneath the hologram." https://www.casascius.com/.
[91] This awareness can help us to imagine, devise and support different futures (Lietaer, 2001 p. 26).

Since the 1990s cryptographers have endeavored to design a system in which digital money tokens could functions over the Internet. Where all attempts that came before proved unsuccessful in the longer term, Bitcoin enjoys sustained interest. When Bitcoin was launched in 2008, it landed amidst the financial crisis that struck in that year. In a time in which public trust in 'big brother' institutions such as governments and banks appears to be low, the critical statements of Bitcoin's designer Nakamoto in his white-paper landed on fertile soil. Nakamoto is critical of the contemporary fractional reserve banking system and the black-boxed monetary policy of central banks, who (s)he accuses of lending out money in arbitrary waves of credit bubbles.

Bitcoin's use of cryptography relates it to the 1990s cypherpunk movement of libertarian cryptographers, who were concerned over personal civil rights and anxious of how 'big brother' could invade privacy on a large scale. Therefore, they tried to make digital cash function over the Internet in a way that preserved privacy. Bitcoin is the latest cryptographic effort, intended as payments inside the Internet sphere at large. This resonates with the cyber-libertarian view of the Internet that was put forward in the 1990s, which argues that this sphere is separate from 'real-space' and above and beyond governments and its laws. Furthermore, Bitcoin appeals to the contemporary worldview of the libertarian political philosophy, which is critical of the nation state and its governments, while it advocates private property and the 'free' market; Bitcoin tokens are pieces of information that are put forward as privately owned objects. In addition, in a way similar to how BitTorrent challenges the established business models of the recording industry, mass adoption of Bitcoin poses a challenge to how governments secure revenue.

The field of economics traditionally describes money by means of its four functions, where the medium of exchange is often treated as the primary function. Bitcoin is presented is a new medium of exchange, where the project's name Bit*coin* points at the intent of the programmers to model cash. Bitcoin is positioned as an 'electronic' analog of cash and more often as 'virtual' cash. I have asked what the term 'virtual' is intended to signify when applied to 'cash'. Furthermore, cash is a rather specific description, instead of a wider categorization such as virtual money or currency. Therefore, I have asked why Bitcoin is said to model cash specifically. The philosophical discussion of the term 'virtual' within the field of new media studies proved irrelevant in the context of Bitcoin, given that 'virtual' is used here

merely to signify that Bitcoin is presented as a model of cash. However, following the argument that Bitcoin is a model, this means that the designers of Bitcoin have interpreted a phenomenon and translated it into a model. . I have argued by means of Lawrence Lessig statement that 'code is law', that code determines what people can and cannot do. In addition, a model is by definition reductive, which indicates that choices have been made in what to include in Bitcoin's code and, more important; what not. I have argued that even if Bitcoin can be said to be in some ways similar to cash, it is important to analyze which properties have been left out, given that choices have been made which enables as well as constrains users. In addition, software architecture codifies values, embedding them in code. Choices have been made which give certain values precedence over others, which points at the political nature of Bitcoin.

Key motivational drivers behind the development of Bitcoin software arose from the criticism of the centralized organization of the contemporary money system, its 'arbitrary' and opaque monetary policy, the fractional reserve banking practice responsible for credit bubbles and the required trust. Nakamoto argues that we should replace trust with cryptographic proof as he "…proposed a system for electronic transactions without relying on trust." (2008, p. 8). However, as Bitcoin is put forward as a model of cash, its designers had to create money tokens in some other way. With Bitcoin, the regulator code takes the place of central bank monetary policy. In doing so, Bitcoin has substituted one power for another, or as Lawrence Lessig puts is: "…one form of power may be destroyed, but another is taking its place." (2006, p. 94). Bitcoin does not succeed in fulfilling Nakamoto's promise of dispensing with the trust that the contemporary money system requires. Trust does not disappear but is established through cryptographic proof via Bitcoin's network politics involving the rule of 'one-CPU-one-vote' and essentially depending on 'honest' nodes that obey the rules. When users adopt Bitcoin they put their faith in its code and the team of six developers, 'buying in' to its protocol including the embedded values that come along with it.

Bitcoin models several aspects of the contemporary money system, such as the limited supply of tokens. Bitcoin's functional likeness to cash is that a Bitcoin seems an independent object that 'changes hands', transferable from person to person. Our contemporary cash tokens appear as independent, stand-alone objects leading lifes of their own in everyday exchange, where the tokens can function for

years in the hands of several people without touching the banking system. Bitcoins are intangible tokens of ciphertext information that in this respect function like cash tokens. Bitcoin adheres to the widely held, but wrong belief that the tangible 'hard' cash *is* money, instead of cash being the credential with which one can prove *title to* money. In other words, cash is the IOU with which the creditor 'you' proves title to the debt of 'I'. Thus, Bitcoin has a functional likeness to *the identifier to money*, cash, rather than that it has a functional likeness to contemporary money itself; the intangible abstract numbers administrated by banks that quantify the concept of debt. Therefore, Bitcoins main difference is that contrary to contemporary currencies such as the euro, Bitcoins are not created as debt relations between legal entities. Instead, Bitcoins are created 'debt-free' , meaning that once Bitcoins have been created (verified) there is no requirement of Bitcoins to be paid back to the issuer as is the case with contemporary money.

In analyzing the differences between Bitcoin and contemporary cash, the goal was not to disqualify Bitcoin opposed to the contemporary money system. On the contrary, although Bitcoin is modest with respect to scale, for an extended period of time it proves functional without critical malfunctions. It functions as cypherpunks have envisioned it since the 1990s; as an Internet payment system in which users participate voluntarily and one that does not rely on enforcement of laws through government coercion. It is unlikely that users can call upon law enforcement in case of losses or fraud, due to Bitcoin's lacking legal entity and the current uncertain legal status of Bitcoins. Perhaps an unforeseen effect of Bitcoin is that its functioning without the concept of debt serves as an eye-opener that there are alternatives to the contemporary organization of money based on debt [92]. Lietaer notes that "By becoming aware of the various money systems and their effects [we are able] to make knowledgeable choices [which] allows us to imagine, devise and support different futures." (2001 p. 26). In the context of the purported crisis of the contemporary money system, I argue in favor of a debate that should unfold focusing on the values embedded in Bitcoin's code and whether we agree on the manner its power is exercised. In other words, does Bitcoin live up to our ideas how money should function in the age of the Internet? Various alternative approaches to concepts of money functional on the Internet are available building on different principles and values[93].

[92] The system that Graeber and Ruskoff call naturalized, that appears as if it is the one possible organization.
[93] For example, where Bitcoin is an argument for money tokens as private property and not through personal (debt)

7. Bibliography

Aftermath Project (2012). *Aftermath Network.* Retrieved from: http://www.aftermathproject.com/filter/aftermath-network/aftermath-network

Baker, S.A. and Hurst, P.R (1998) *The Limits of Trust: Cryptography, Governments, and Electronic Commerce.* Boston: Kluwer Law International, xv

Barlow, J.P. (2000 October 10). *The Next Economy of Ideas.* Retrieved from: http://www.wired.com/wired/archive/8.10/download.html

Bell, J. (1992). *Assassination Politics.* Retrieved from: http://www.outpost-of-freedom.com/jimbellap.htm

Bitcoin.org (2012). *Bitcoin P2P Digital Currency*. Retrieved from: http://bitcoin.org/

Bitcoin Basics (2012). *Introduction.* Retrieved from: https://en.bitcoin.it/wiki/Introduction

BitcoinStats (2012). *Transcript for #bitcoin-dev 2011/04/26 page 5.* Retrieved from: http://bitcoinstats.com/irc/logs/2011/04/26/5#l445170

Castronova, E. (2005) *Synthetic Worlds.* Chicago: The University of Chicago Press

Casascius (2012). *Physical Bitcoins By Casascius.* Retrieved from: https://www.casascius.com/

Cohen, N. (2011 July 3). *Speed Bumps on the Road to Virtual Cash.* Retrieved from: http://www.nytimes.com/2011/07/04/business/media/04link.html?_r=1

relations, the Ripple Project software alternatively builds on the concept of money as promises between people, through credit relations and IOU's (Ripple Project, 2012)

Deleuze, G. (1994). *Difference and Repetition.* New York: Columbia University Press

Diablo III Action House FAQ (2012). *Diablo III Beta Announcement.* Retrieved from: http://us.blizzard.com/en-us/company/events/diablo3-announcement/index.html#auction:auction-faq

Dibbell, J. (2006). *Play Money: or, How I Quit My Day Job and Made Millions Trading Virtual Loot*. New York: Basic Books.

Dictionary (2012). *Virtual.* Retrieved from: http://dictionary.reference.com/browse/virtual

Dolland, C. (2012 March 2). *Ron Paul Lectures Ben Bernanke on Real Money*. Retrieved from: http://www.opencurrency.com/ron-paul-lectures-ben-bernanke-on-real-money/

ECB (2012). *Balance Sheet.* Retrieved from: http://wwwecb.europa.eu/press/pr/wfs/2012/html/fs120710.en.html

FBI (2012). *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity.* Retrieved from: http://cryptome.org/2012/05/fbi-bitcoin.pdf

Genesis Block (2012). *Main network genesis block*. Retrieved from: https://en.bitcoin.it/wiki/Genesis_block

Goldsmith, J. and Wu, T. (2006). *Who Controls The Internet? Illusions of A Borderless World.* Oxford: Oxford University Press

Graeber, D. (2011). *Debt: The First 5,000 Years*. Brooklyn, N.Y: Melville House.

Grinberg, R. (2011). Bitcoin: An Innovative Alternative Digital Currency http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857

Grishchenko, V. (2011 May 12). *Bitcoin?* Retrieved from: http://www.pds.ewi.tudelft.nl/~victor/bitcoin.html

Guttmann, R. (2003). *Cybercash: the coming era of electronic money.* New York: Palgrave Macmillan

Lastowka, G. (2010). *Virtual Justice – The New Laws of Online Worlds.* New Haven and London: Yale University Press

Hamacher, K. and Katzenbeisser, S. (2011). *Bitcoin – An Analysis [28C3]*. Retrieved from: http://www.youtube.com/watch?v=-FaQNPCqG58

Hayles, N. K. (1999). *How we became posthuman: Virtual bodies in cybernetics, literature, and informatics*. Chicago, Illinois: University of Chicago Press.

Heeks, R. (2010). *Understanding "gold farming" and real-money trading as the intersection of real and virtual economies.* Journal of Virtual Worlds Research *2*, no. 4. Retrieved from: http://journals.tdl.org/jvwr/article/viewArticle/868

Hughes, E. (1993). *A Cypherpunk Manifesto*. Retrieved from: http://www.activism.net/cypherpunk/manifesto.html

Hulsebosch, P. (2012 June 13). *Real money auction house uit Diablo II gaat van start.* Retrieved from: http://tweakers.net/nieuws/82535/real-money-auction-house-uit-diablo-iii-gaat-van-start.html

Ithaca Hours (2012). *What are Ithaca Hours?* Retrieved from: http://www.ithacahours.org/

Jackson, E.M. (2004). *The PayPal Wars: Battles With Ebay, the Media, the Mafia, And the Rest of Planet Earth.* Los Angeles, CA: World Ahead Publishing

Lessig, L. (2006) *Code version 2.0.* New York: Basic Books. Retrieved from: http://codev2.cc/

Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*.

New York: Penguin Group

Lietaer, B. A. (2001). *The Future of Money: Creating New Wealth, Work and a Wiser World.* London: Random House

Lister, M., Dovey, J., Giddings, S., Grant, I. And Kelly, K. (2009). *New Media: A Critical Introduction.* Second edition. New York: Routledge

Matonis, J. (2012). *Monetising Gameplay on Social Network Sites.* Retrieved from: *http://www.slideshare.net/jonmatonis/monetising-game-play-on-social-network-sites*

McLuhan, M. (1964). *Understanding Media.* New York: Routledge

Nakamoto, S. (2008). *Bitcoin: a Peer-to-Peer Electronic Cash System.* Retrieved from: http://bitcoin.org/bitcoin.pdf

Nakamoto, S. (2008 November 14). *Re: Bitcoin P2P e-cash paper.* Retrieved from: http://www.mail-archive.com/cryptography@metzdowd.com/msg10001.html

Nystrom, C. L. (1973). *Toward a science of media ecology: The formulation of integrated conceptual paradigms for the study of human communication systems*. Doctoral dissertation, New York University, 2001.

Onion, The (2010). *U.S. Economy Grinds to Halt as Nation Realizes Money Just A Symbolic, Mutually Shared Illusion.* Retrieved from: http://www.theonion.com/articles/us-economy-grinds-to-halt-as-nation-realizes-money,2912/

P2pfoundation (2012). *Bitcoin.* Retrieved from: http://p2pfoundation.net/Bitcoin

Peck, M.E. (2012). *Bitcoin: The Cryptoanarchists' Answer to Cash.* Retrieved from:

http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/0

Poulsen, K. (2010 December 4). *PayPal Freezes WikiLeaks Account.* Retrieved from: http://www.wired.com/threatlevel/2010/12/paypal-wikileaks/

Reid, F. and Harrigan, M. (2011). *An Analysis of Anonymity in the Bitcoin System.* Retrieved from: http://arxiv.org/abs/1107.4524

Ripple Project, The (2012). *The Ripple Project.* Retrieved from: http://ripple-project.org/

Rushkoff, D.M. (2012). *Monopoly Moneys: The media environment of corporatism and the player's way out.* Doctoral dissertation, Utrecht University

Schaefer, M.T. (2008). *Bastard Culture! How Users Participation Transforms Cultural Production.* Retrieved from: http://mtschaefer.net/entry/bastard-culture-how-user-participation-transforms-cultural-production/

Schroeder, J.L. (2012). *Cold Cash: The Fantasy of Real Money.* Cardozo Legal Studies Research Paper No. 361. Retrieved from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2026108

Stanford Encyclopedia of Philosophy (2012). *Libertarianism*. Retrieved from: http://plato.stanford.edu/entries/libertarianism/

Van Den Boomen, M., Lammes, S., Lehmann, A., Raessens, J. and Schaefer, M.T. (2009). *Digital Material: Tracing New Media in Everyday Life and Technology.* Amsterdam: Amsterdam University Press

Wallace, B (2011 November 23). *The Rise and Fall of Bitcoin.* Retrieved from: http://www.wired.com/magazine/2011/11/mf_bitcoin/all/1

Wikipedia (2012). *List of things described as virtual.* Retrieved from:

en.wikipedia.org/wiki/List_of_things_described_as_virtual