IJCCR

www.ijccr.org · ISSN: 1325-9547

Jansen, M. (2013). Bitcoin: The Political 'Virtual' Of An Intangible Material Currency. *International Journal of Community Currency Research 17*, 8-18.
https://doi.org/10.15133/j.ijccr.2013.002

International Journal of Community Currency Research

VOLUME 17 (2013) SECTION A 8-18

BITCOIN: THE POLITICAL 'VIRTUAL' OF AN INTANGIBLE MATERIAL CURRENCY

M. A. Jansen*

Faculty of Humanities, Utrecht University

ABSTRACT

This paper concerns the open source software project Bitcoin, which is often described as virtual cash. The paper investigates what 'virtual' signifies when applied to 'cash' and in turn what 'virtual cash' says about Bitcoin. Bitcoin is the latest cryptographic effort to create digital cash-like tokens, where Bitcoin's designer Nakamoto argues that users now no longer have to trust a third party, traditionally the bank. Paradoxically, for Bitcoin it is key that nodes in the network agree on the status of the shared block chain database. 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, its function as a credential referring to debt. Bitcoin discontinues the concept of debt.

* Email: info@markajansen.nl

To cite this article: Jansen, M. (2013) 'Bitcoin: The Political 'Virtual' of an Intangible Material Currency' *International Journal of Community Currency Research* 17 (A) 8-18 <www.ijccr.net> ISSN 1325-9547

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 allegedly catastrophic cascading failures elsewhere in the banking system in case these banks in the category 'too big to fail' would declare bankruptcies. Currently, several European countries such as Greece, Spain, Portugal and Italy are in a debt crisis, having difficulties getting government finances in order. 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). Already in 2001, former central banker Bernard Lietaer wrote in his book *The Future of Money* that "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).

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, 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 software 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, however so far Bitcoin is an exception. Bitcoin enjoys increasing interest after the project 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' that was held by some as a precedent-setting type of censorship (Poulsen, 2010)

Various authors have explored what money might be like in the Internet sphere. Bernard Lietaer in his book *The Future of Money* argues that "Money is modem society's central information system", hinting at the compatibility of money and the Internet (2001, p. 22). Professor of economics Robert Guttmann in his book C*ybercash: 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). 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, '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 why the programmer of Bitcoin and several journalists and other critics 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. The result of this analysis are insights into the similarities but also the discontinuities between contemporary money and Bitcoin.[1]

The reader might note that it is not conventional to approach money as a medium. However, already in 1964 Marshall McLuhan, famous for stating that 'the medium is the message' and coining the term 'global village', 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, commodity and currency. 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. 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. Bitcoin is an experimental open source software project, which facilitates the exchange of Bitcoins (BTC). 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

[1] For an extended analysis please refer to the Masters Dissertation on which this paper draws. Available from: http://igitur-archive.library.uu.nl/student-theses/2012-0906-200953/UUindex.html

founded almost 90 years ago as a result of a credit crunch and global financial instability, invoking a sense of deja vu looking at the contemporary financial context of Bitcoin. Complementary currencies such as WIR and Ithaca Hours are local efforts and often have the goal of keeping local money local (Ithaca Hours.org, 2012). In contrast, in a way similar to the file-sharing software BitTorrent, Bitcoin enjoys global scalability, enabling instant payments to anyone, anytime, anywhere in the world (Bitcoin.org, 2012). 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 go without 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 as well as transactions are carried out collectively by the network following a protocol. On the P2P Foundation wiki Nakamoto is quoted saying 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 *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.* (2012, emphasis added)

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*." (p2pfoundation, 2012 emphasis added). 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 added):

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 the contemporary institutions that manage the financial system - banks. Nakamoto makes the core motivations for the development of Bitcoin very clear, these being the mistrust of so-called 'big brother' institutions that do not provide financial privacy. In the code of the genesis block, the first block of Bitcoin transaction information, Nakamoto 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 the contemporary fractional-reserve banking practice (Genesis block, 2012). Other motivations include possible censorship by disallowing organizations to participate in the system, such as the widely publicized Wikileaks' Banking Blockade. 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. (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; Bitcoin arguably removes the trusted third party and allows users to transact directly with each other.

Nakamoto states that Bitcoin has no centralized authority, unlike the central bank-managed contemporary currencies such as the euro. 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 method is important to understand, given that its technical rationale is informed by Nakamoto's economic philosophy and determines the pre-distribution of Bitcoins. 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 [2]

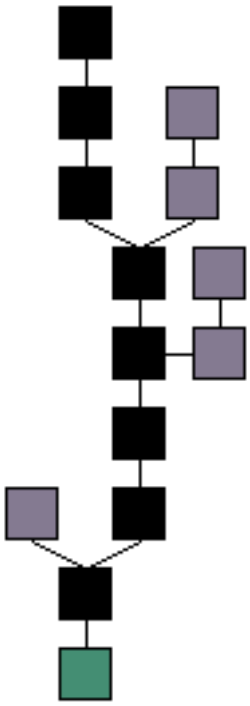

Figure 1. Visualization of Bitcoin's block chain. The main chain (black) consists of the longest series of blocks from the genesis block (green) to the current block. Orphan blocks (grey) exist outside of the main chain.
Source: http://en.wikipedia.org/wiki/File:Blockchain.svg

Bitcoin creation 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'. The software searches for a solution to a mathematical problem whose difficulty is precisely known. 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 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. The block chain is how Bitcoin solves the 'double-spending problem' that is prevalent in a digital environment wher 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 a single party acting as central hub authority. Thus, all Bitcoin transaction information is public, including transaction 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. 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). 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).

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. 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 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 fee. Although Bitcoins in principle can be send without any transaction costs, senders of Bitcoins may 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. Furthermore, there is no rule that ensures that transactions get processed; miners are in principle free to include some transactions in a block while leaving others unattended.

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 pay-

[2] For a more elaborate technical analysis I refer the reader to Nakamoto's whitepaper *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008).

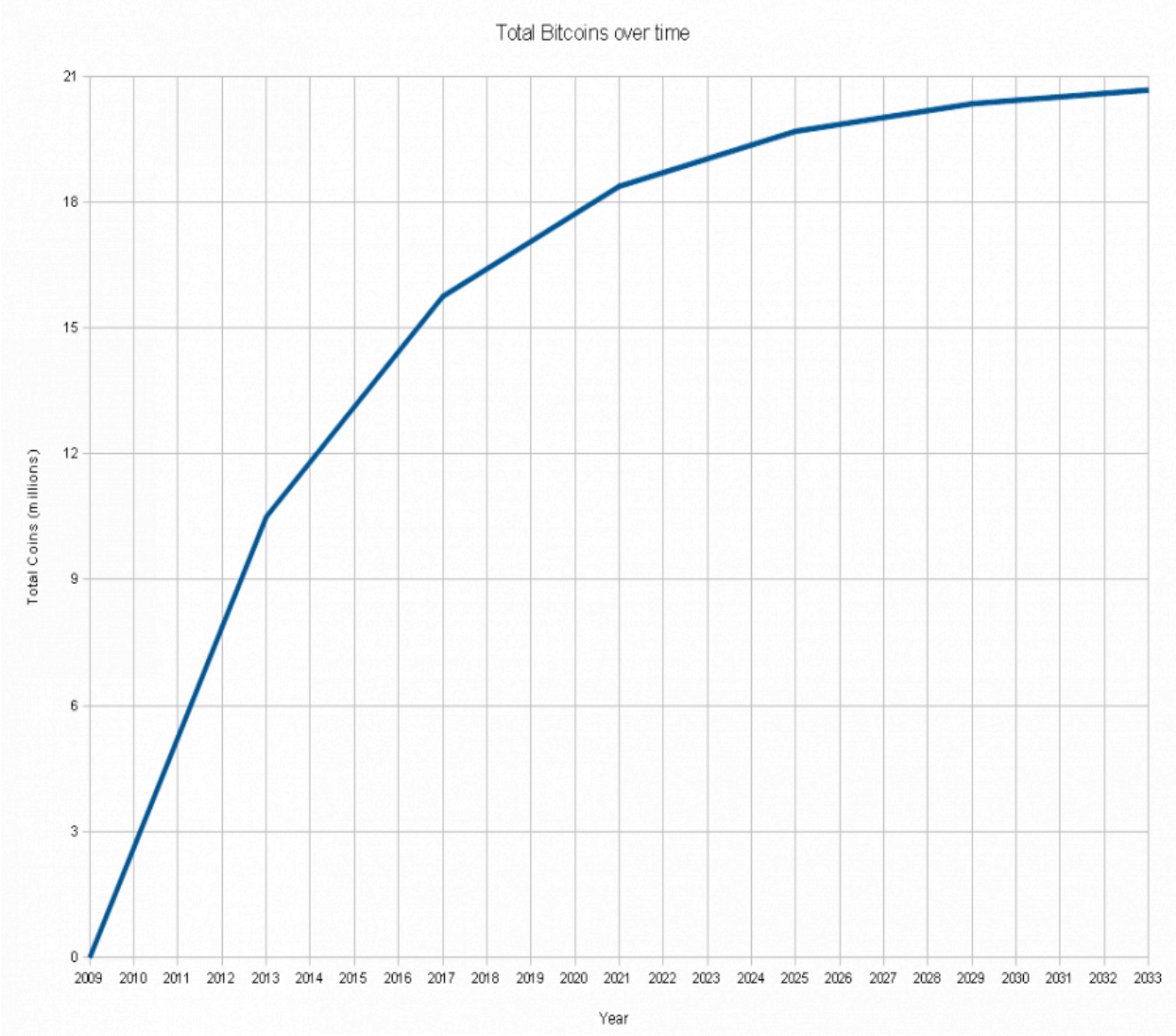

Figure 2. Total Bitcoins over time. Source: http://zh.wikipedia.org/wiki/File:Total_bitcoins_over_time.png

ments over a communications channel without a trusted third party." (Nakamoto, 2008 p. 1). Given Nakamoto's desire to remove trust in an intermediary party, for Bitcoin a paradoxal key issue is whether trust can be established among the nodes in the network. Nakamoto asserts "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). 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', where those who control more CPU/GPU's command more power.

The mathematical difficulty of Bitcoin verification increases as more nodes participate in the process, thus 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, popularly referred to as Bitcoin mining 'farms' or 'supernodes'. Therefore, in contrast with Nakamoto's argument that Bitcoin is completely decentralized, 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).

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

Nakamoto's claim that Bitcoin is completely decentralized is overrated; a utopian statement very much similar to the myth that the Internet completely disposes of intermediaries, were it often also creates new ones.[3] Furthermore, I noted earlier that miners choose which transactions to process. Although it appears that most miners are 'nice' in the sense that they also include transactions that do not yield transaction fees, this also suggests that not all nodes in the p2p network are equal but rather that some are more equal than others. Interestingly, what emerges in Bitcoin practice is something not completely unlike the contemporary financial system.

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. Bitcoin through its protocol functions different from contemporary intermediaries, however it does not fulfill Nakamoto's promise that with Bitcoin there no longer is a trusted third party, because the protocol remains the intermediating mechanism through which users interact. Trust does not disappear but it shifts from the former intermediary to the next, from bank to Bitcoin's protocol. 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 its code. This amongst others entails that users accept and 'buy into' the arbitrary limit of 21 million Bitcoins, the one-CPU-one-vote rule and the resulting network politics of supernodes that have more power than average users with more common computer hardware.

In the next paragraph I will go into Bitcoin's 'virtual' aspect. The name 'Bitcoin' 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 a critique of theory from experts on the economies of virtual worlds.

3. POLITICS OF THE 'VIRTUAL'

Nakamoto and others often describe Bitcoin as 'virtual cash', however they do not explain why they choose to describe Bitcoin by means of the term 'virtual', or what this term signifies in relation to both cash and Bitcoin. The term

[3] In the financial context of Bitcoin, exchanges like Mt. Gox are examples of new intermediaries.

'virtual' has a long history, originating from Medieval Latin *virtuālis*, meaning "influencing by physical virtues or capabilities" (Dictionary, 2012). 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). The wiki states 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 added).

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'. The 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 is an intangible that resists touch and seems ephemeral. 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 adds 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).

The term 'virtual' is often used to describe Bitcoin as virtual cash, to communicate that Bitcoin is in some respects like cash. In a way similar to how Szabo explains that *bit gold* was designed to mimic certain characteristics of gold, Bitcoin is designed to be an intangible model of cash working over the Internet. Interestingly, Nakamoto also draws analogies between the Bitcoin verification process and gold mining. Bitcoin is put forward as mimicking aspects of both cash and gold. However, in stressing similarities we should not forget that Bitcoin might also in some respects differ from the modeled phenomenon. 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. Lawrence Lessig, professor of cyberlaw, stresses the 'politicalness' of software design as he argues that "code is law":

> 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). Lessig illustrates this by means of an example, 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). Software architecture programs values in code. Ultimately, the code is what determines the environment in which users interact. In addition, in MMOG 'space' the possibilities are not only determined by code, but in addition the metaphorical 'space' itself also consists of code. Given that these 'spaces' increasingly form the environment in which people work, play and live, the political power of those able to read, edit and write code is obvious, as this is what shapes the rules of interaction in digital contexts.

In his book *Synthetic Worlds,* virtual world economist Edward Castronova argues in line with Lessig that the code of MMOG's determines what is possible and what is not. Castronova validates that a programmer, which he refers to as the 'coding authority', makes choices with regard to what code will and will not permit. Castronova writes the following about the volume and availability 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. … The availability of diamonds is not an endowment but a choice. Thus while the men-

> tal 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)

Bitcoin's 'endowment' is the result of many choices made by its programmers between possible alternatives. For example, the maximum volume of Bitcoin's that are allowed to exist is set to an arbitrary limit of 21 million. Through code this arbitrary constraint becomes a voluntary endowment for users who accept the system. It is important to note that this observation also holds for contemporary money, given that monetary policy determined by central banks forms the basis for the endowment of money that 'users' have to accept. Given that money occupies an important position within economics, Castronova in his text also touches upon what gives value to money in 'real' space. 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 added)

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 coding authorities and visual 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 to the observer; gold in WoW is money because it persuasively seems to perform 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 identical to snail mail, or that neither table foosball nor the soccer simulation game FIFA 12 is identical to the sport of soccer that it models.

Castronova asserts that no model is perfect, but that this is not a problem, since only that what matters for the exercise in question, matters for the simulation. This circular logic assumes that 'that what matters' is clear and uncontested. However, the coding authority has determined what matters and, maybe more important, that which does not. Therefore, I suggest that; 1. we should ask "*who decides* what 'matters'?", and; 2. To determine what matters is a political act that shapes which values are awarded precedence as these are embedded in code. In his book *Play Money*, journalist Julian Dibbell disposes of questions such as these, which he calls unnecessary and time-wasting 'ontological' questions. Dibbell agrees with Castronova that:

> "…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)

I do not consider it problematic that Bitcoin is 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. The key insight here is that in stressing the similarities of the 'model' to that which it is modeled after, not enough attention remains to discuss differences.

By definition a model is presented as a simplified, reductive representation of (a part of) perceived reality. Hence, inherent to a model is that not all properties or dimensions are included. Thus, we can assume that the simulation overall does not function in exactly the same way. In other words, Bitcoins and 'gold' in virtual worlds are in many ways not like the money in your pocket. In addition, models are not neutral, but *contested*, or at least contestable. What 'matters' is not pre-given but determined by 'authorities'. This obscures that what supposedly does not matter and shoves what is left out of the model under the veil of the 'virtual'. In case of Bitcoin we should not even expect perfect exactitude, given that Nakamoto is critical of certain aspects of the system that (s)he models. In other words, if Bitcoin would be a perfect copy nothing would be different and Bitcoin would just be more of the same, which is probably 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. We should contest the 'ontology' of the model, debate what we deem important enough to include and what not. Without analyzing beyond face value, or rather *interface value*, without asking what is different, we might unknowingly award certain values precedence over others.

Now I have discussed the 'virtual' of Bitcoin and argued that Bitcoin is not the same as cash, it is also important to review what 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. 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.

4. CONTEMPORARY MONEY SYSTEM

The contemporary money (€) system in the European Union is organized by central and commercial banks, managed through the principles of accounting and the fractional-reserve banking practice. 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. 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. Via monetary policy, the central bank determines the volume of what is known as 'base money', often through loans to the government. 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 Euro-currency system, to state in his book *The Future of Money* that "Money is modern society's central information system (2001, p. 22).

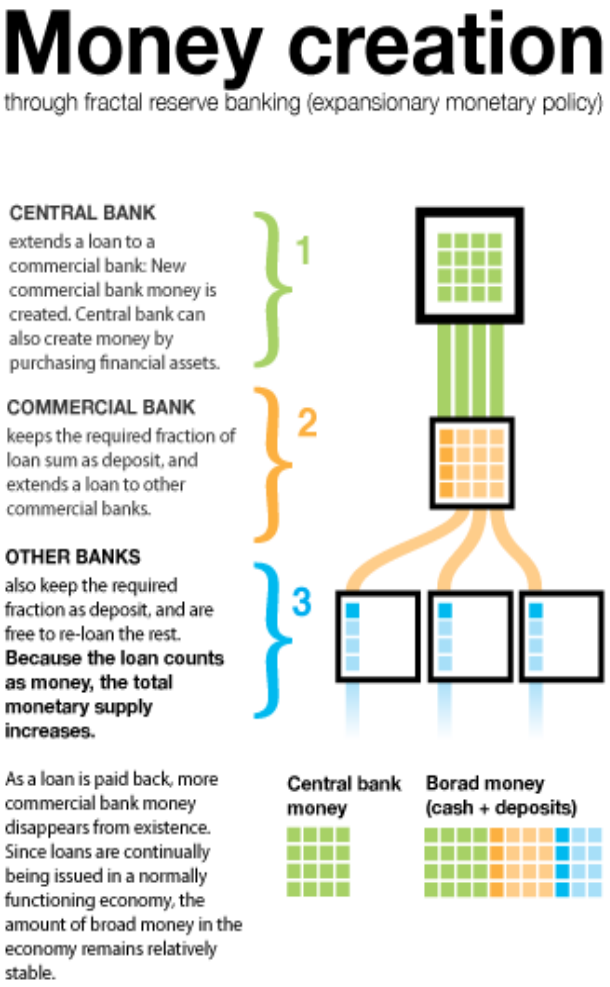

Figure 4. Money creation via the fractional reserve banking practice. Note: 'borad money' is a typo, which should be 'broad money'. Source: http://upload.wikimedia.org/wikipedia/commons/f/f2/Money-creation.gif

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. 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 a new amount of new money based on the rest of the amount. The fractional reserve banking practice increases the money supply, and banks are said to create money. Due to fractional reserve banking, the broader money supply is a multiple of 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 money in "…waves of credit bubbles *with barely a fraction in reserve.* (2008, p. 1 emphasis added). The Bitcoin report by the FBI validates that "…central banks can *arbitrarily* increase the supply of currency…" (FBI, 2012 emphasis added).

Nakamoto is correct that commercial banks can extend credit in excess of deposits. However, the statement that banks should have something 'in reserve' refers to the notion of how banks operated at a time back in history, where customers would deposit objects like gold with a bank and get a receipt, an IOU, which would circulate like cash money does today. However, this is not how the contemporary money system operates; (central) banks can have assets on their balances such as gold, but in effect they have nothing 'in reserve' but the registration system that provides information about debits and credit, and assets and liabilities. In other words, if an EU citizen takes her Euro's to the central bank, the bank is not legally obliged to provide anything other in return for one Euro than another Euro. Furthermore, Nakamoto is also correct that central bankers can increase the supply of money, as bankers have no set goal of keeping the supply under a certain threshold – instead the ECB targets a rate of inflation, meaning aggregate price levels. In other word, there is no pre-determined 'right' money volume and I have shown that volume is just as arbitrary with Bitcoin's limit of 21 million. Given that Bitcoin is specifically positioned as a digital model of cash, I will now go into the status of cash in the contemporary money system.

Cash is a standardized credential that provides authentication to a bank that the bearer of the note or coin has valid title to the credit administered by banks. 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 as 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. In other words, intangible Bitcoin tokens in fact model the credential function of the tangible cash tokens that in the contemporary system function as proof of title to intangible money 'in the book's'. As argued earlier, Bitcoins are not created as debt but via the verification process I described in section 2 above. Where the contemporary money is self-referential, Bitcoins refer to nothing as they are created and predistributed as transactions without a source. Different from contemporary money based on debt relations, Bitcoin tokens exist independently as privately owned cryptographic tokens, as cyphertext information 'objects' in the network. Thus, Bitcoins are conceptually very much different from cash, which refers to and could not exist without the debt relations of bank bookkeeping. Lietaer asserts that the belief that money is a tangible object is "…a key illusion in the magic about money" (2001, p. 46).

To conclude, the goal of this analysis was neither to disqualify Bitcoin as opposed to contemporary money, nor 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)[4]. 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). Bitcoin-as-alternative may assist in realizing a perceptual shift, as a new lens that helps us to see, revealing the structural biases of an ancient naturalized medium that until now remained largely invisible as it quietly but consistently ran in the societal background. 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.[5]

BIBLIOGRAPHY

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

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

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

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

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

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

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

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

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

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

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

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

[4] 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.

[5] For example, where Bitcoin is an argument for money tokens as private property, the Ripple Project software alternatively builds on the concept of money as promises between people, through credit relations and IOU's; as information about personal (debt) relations (Ripple Project, 2012)

Lister, M., Dovey, J., Giddings, S., Grant, I. And Kelly, K. (2009). New

Media: A Critical Introduction. Second edition. New York: Routledge

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 conceptualparadigms for the study of human communication systems. Doctoral dissertation, New York University, 2001.

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/

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/

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