

Bitcoin, the end of the Taboo on Money

Denis Jaromil Roio, Planetary Collegium Ph.D. candidate, M-Node

6 April 2013, version 1.0

Abstract: Bitcoin is a decentralized system of digital authentication that facilitates the circulation of value on the Internet without the presence of any intermediaries, a characteristic that has often gained it the definition of “digital cash” or “crypto currency”, since it can be used as money for payments. This article consists in a technoetic inquiry into the origins of this technology and its evolution. This inquiry will take in consideration the biopolitical dynamics that govern the Bitcoin community as well specific characteristics of the technical realization, aiming to provide insights on the future of this technology as well a post-humanist interpretation of its emergence.

Keywords: Bitcoin, Crypto, Currency, Digital, Network, Community, Technoetic

Contents

1 Acknowledgments	2
2 Introduction	3
3 Origins	3
4 Memorable events	4
5 Innovation	5
5.1 Networked computing	5
5.2 Why mining	6
5.3 Accounting science	6
6 Community	8
7 Passion	10
8 Glory	12
9 Popularity	14
10 Conclusion	15
11 Contributor details	16
12 References	17

1 Acknowledgments

Bitcoin, the end of the Taboo on Money

from the DYNDY.net article series

© 2013 Dyne.org Digital Press

E-mail: <press@dyne.org>

Author: Denis Roio aka Jaromil

Peer reviewed by: Christian Nold, Susanne Jaschko, Debra Solomon, Marco Sachy, Amir Taaki

Revisions:

- 6 April 2013 - first public edition

The original source of distribution for this article, also providing its most up to date version, is the Internet website <http://jaromil.dyne.org/writings>

This content is licensed as Creative Commons "BY-NC-SA" 3.0 in the jurisdiction of the Netherlands: it is free to be copied, republished for non-commercial use, quoted and remixed by providing correct attribution to its author(s), while all derivative works must adopt the same license. Different licensing conditions can be arranged, those interested can write to Dyne.org Press <press@dyne.org>

Please support free publishing donating Bitcoins to 1LwSugK8X8kRpV3sex9f8KTjVPc52FPaEq

More ways to donate are available, see <http://www.dyne.org/donate>

ENGLISH LICENSE TEXT (TRANSLATION)

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Netherlands License. To view a copy of this license (english translation), visit <http://creativecommons.org/licenses/by-nc-sa/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

DUTCH LICENSE TEXT (ORIGINAL)

Dit werk is gelicenseerd onder een Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen 3.0 Nederland. Bezoek <http://creativecommons.org/licenses/by-nc-sa/3.0/nl/> om een kopie te zien van de licentie of stuur een brief naar Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

2 Introduction

The most powerful forces, those that interest us the most, are not in a specular and negative relation to modernity, to the contrary they move on transversal trajectories. On this basis we shouldn't conclude that they oppose everything that is modern and rational, but that are engaged in creating new forms of rationality and new forms of liberation.

Negri and Hardt, 2010, "Commonwealth"

This article doesn't aim to describe what Bitcoin is to the reader: there are several information sources that already accomplish that, starting from well designed video animations¹, vast numbers of press and academic articles listed on the wikipedia entry², and even a rather positive dramatization in an episode of the popular TV series "The Good Wife"³.

Rather than divulging the functionality of Bitcoin or its vulnerabilities, or even building an interpretation of it according to economic theories, this article investigates historical and philosophical aspects related to the emergence of this technology. In order to do so, the writer has been involved for more than two years within the Bitcoin community, engaging in both cooperative and critical exchanges with its peers.

Money is a fundamental medium upon which to build constituency and consolidate sovereignty. This research investigates the need for such a constituency, its urgency and emergence as a form of subjectivation. Ultimately this article provides a picture of the cultural context in which Bitcoin was grafted and has grown up to what it is now, offering keys to interpretation of its social and political aspects.

3 Origins

In 1994, almost two decades ago, a vast amount of time for the rythms of digital life, Steven Levy published in Wired an article titled "E-Money (That's What I Want)"⁴ with an introduction that left no doubts to the reader:

"The killer application for electronic networks isn't video-on-demand. It's going to hit you where it really matters - in your wallet. It's, not only going to revolutionize the Net, it will change the global economy."

For those who don't know Steven Levy, author of books like "Crypto" or "Hackers", let me just say that he is not the visionary type: his writings contain very little fantasy at all, and follow a journalistic approach in documenting the stories he investigates. In this article he voices the case of David Chaum "the bearded and ponytailed founder of DigiCash" who was working in Amsterdam to "catapult our currency system into the 21st century". In fact almost 20 years ago David Chaum was a researcher in the CWI, the national research institute for mathematics and computer science in the Netherlands, where in recent times I've had the honor to explain how Bitcoin functions⁵ in front of an audience of scientists that have worked with Chaum and, who honestly made me feel quite embarassed until I understood modesty is definitely one of their qualities.

Because I would like to start this article with an historical perspective, I can't help but track the origins of the evolution that Bitcoin represents into circumstances so well debunked in Levy's article, which once again was absolutely ahead of its time.

But that's not all. Bitcoin is not just "digital cash". Its birth and growth has been fostered by a network of trust that, to some degrees, shared ethical principles and the gestation of a constituency: I'm talking about hackers.

Bitcoin first appeared to the eyes of the hacker community in a Slashdot post⁶ which, on August 2010, announced the release of version 0.3. Previous to that, Bitcoin was only known on some minor cryptographer's mailinglist

¹Video introduction to Bitcoin "We Use Coins" <http://www.weusecoins.com>

²References for the Bitcoin entry on Wikipedia <http://en.wikipedia.org/wiki/Bitcoin#References>

³The Good Wife TV series on CBS, season 3 episode 13, recap: <http://blogs.wsj.com/speakeasy/2012/01/16/the-good-wife-season-3-episode-13-bitcoin-for-dummies-tv-recap/>

⁴Levy's article on Wired: <http://www.wired.com/wired/archive/2.12/emoney.html>

⁵Software Freedom Day, 2011, video recording online here: <http://www.youtube.com/watch?v=hdNRw-LWDUY>

⁶Slashdot post on <http://news.slashdot.org/story/10/07/11/1747245/Bitcoin-Releases-Version-03>

which as of today stopped to function. The post I'm mentioning announced the birth of a software that, through the distributed work of all on-line participants, would have created some unique "hashes" which could then be interchanged as "digital cash". Hackers at that time were already familiar with this concept as a similar implementation was circulating already for using a so called "hashcash" to fight spam online, basically putting a computational price on every email server willing to exchange emails. Also the distributed, or clustered architecture of this software sounded familiar, since many of us thought this would be some kind of SETI@Home, a software that distributed the computational work needed to analyze signals from outer space gathered by NASA observatories.

4 Memorable events

In two and a half years following the presentation to the hacker community at large, I'm individuating 2 memorable events that will help us understand Bitcoin's historical progression.

- January 2011 Wikileaks financial blockade
- 9 May 2011 Forbes publishes its first article on Bitcoin

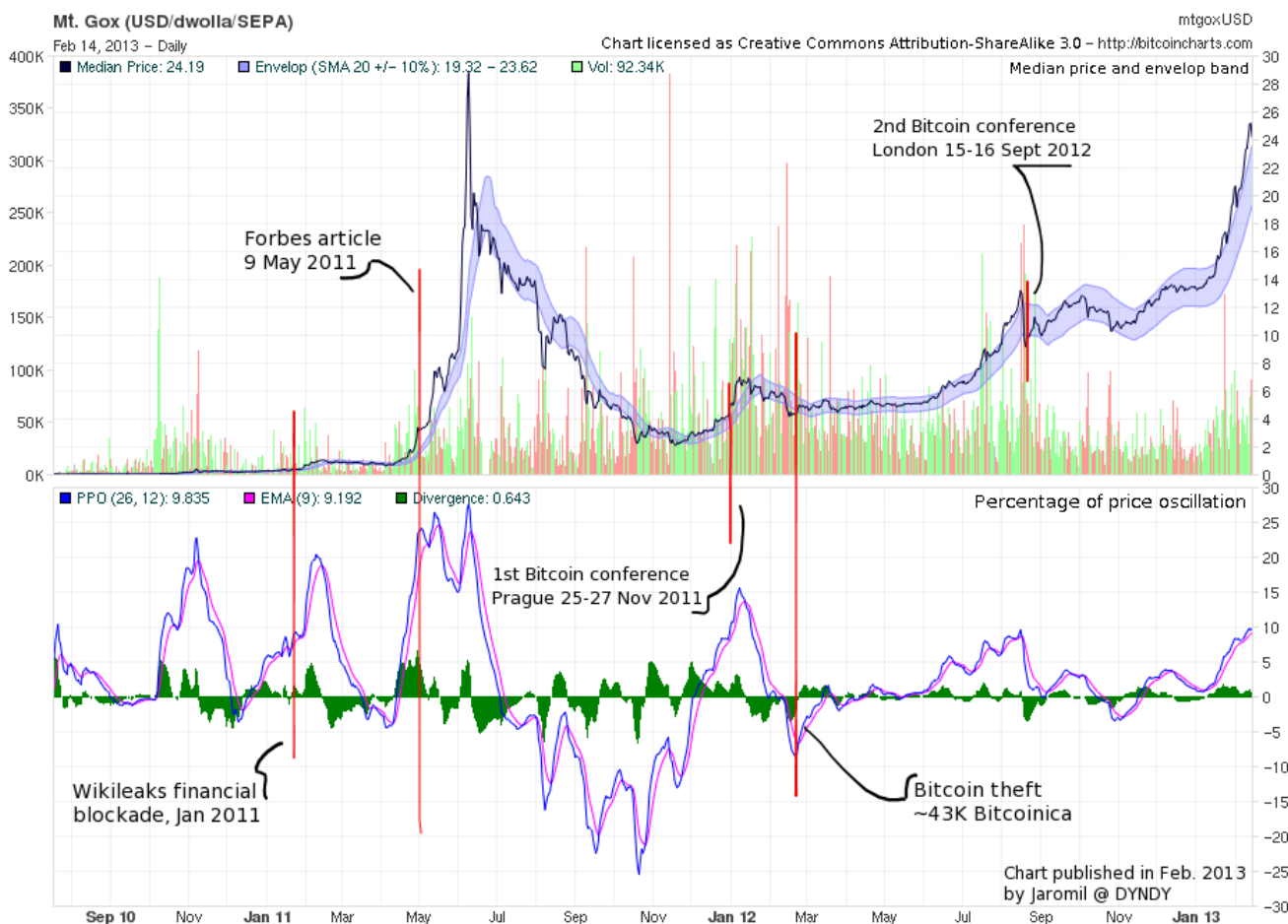


Figure 1: Price graph of memorable events

In *Figure 1* we overlap the chronology of these events to a graph showing the exchange rate of dollar vs Bitcoin on its biggest market "MtGox". The graph is doubled: above is the average exchange value and below is the

percentage of oscillation of the price. This graph helps to outline the influence that socially relevant events have on Bitcoin's financial values.

In the rest of this article I will refer to these two events, trying to explain the complex relationships that govern social and political aspects of Bitcoin. The chart in Figure 1 is probably as close as I'll get in linking such relationships to *financial phenomena*, because as abstract models of human action they have very little importance in my enquiry.

My ambition is to describe Bitcoin's technopolitical innovation without following universals - such universals as those populating most academic disciplined views in *economy*.

Hence, I declare the method of this analysis as *biopolitical*, in the sense that Michel Foucault gave to this word: the early genealogy of a new ethical sense, an enquiry into its gestation phase through the analysis of its processes of subjectivation. *This is Post-humanist Economics*.

5 Innovation

5.1 Networked computing

The physical property of symbols influences decisively the structure of the codes. It is influenced more by this than by the criterion of meaning. The structure of a message reflects the physical character of its symbols more than the structure of the universe it communicates. This explains the famous sentence "The medium is the message".
Vilém Flusser

First of all we need to better explain to the reader what networked computing actually is, a concept to which we'll also refer as clustering.

Clustering is a way to approach problems that are too big to be solved by a single computer, because for instance they require too much computation over a too wide range of data. Clustering a problem means to break it into smaller chunks and then to distribute these chunks to different computer units which all work towards the common goal, such that everyone does a part. It also means that those computers that have less to do, for instance because they are not used at certain moments, can autonomously offer their help to the cluster network that are a part of. One can imagine the situation in which, in a single room with 10 computers, only 5 are being used, those few users can benefit from a faster performance thanks to clustering.

This is no science-fiction, nor a brilliant new idea, although it has been never implemented on the consumer market, probably because it doesn't makes a profit for hardware or software manufacturers. Still, back in 2001, when we published the free operating system Dyne:bolic⁷, its clustering feature, implemented via the Linux kernel patch called OpenMosix, was one of the most appreciated by its users. The feature was announced with the slogan *El computador unido jamas sera' vencido* and it let people accelerate onerous tasks on slow computers (i.e. 3d renderings) by sharing the computational load amongst multiple machines: a perfect situation for grass-roots media-labs that have no money to buy computers and, rather than upgrading their hardware, tend to rely on the number of cheap units that they can recycle from the trash and donations.

The OpenMosix cluster implementation in Dyne:bolic is just an example of how networked computing relates to the economical and political aspects of digital societies. Out of the digital and back to the physical world, the mode of production and distribution of resources in networked computing is extremely relevant for the "energy grid" contemporary discourse.

Back to Bitcoin, while we individuate a clustering architecture in its implementation of a proof of work, we are still far from comprehending the real value that backs Bitcoins. In fact, the kind of work required to "mine" Bitcoins is very far from being connected to real life values: looking for particular numbers whose hashes start with 6 zeros, to make it simple, is nothing more than a quest for numbers.

We need to dig further than that to understand the sense of Bitcoin mining and dispel some legitimate doubts about it being a waste of energy. While its networked computing approach was appealing (hackers inherently love to "cluster things") it is hard to be immediately convinced about the real value of such an operation: only a

⁷The dyne:bolic GNU/Linux OS homepage is <http://www.dynebolic.org>

few initially understood why one should run such an algorithm to transform electricity and tech gear in somehow spendable numbers.

5.2 Why mining

Mining is the act of creating Bitcoins, basically the act of finding this “algorithmical mineral” and minting it into usable tokens. The process of mining is therefore remunerative for those who challenge it, by running the Bitcoin mining software on their computers. In simple terms, mining transforms electricity into Bitcoins: computers look for numbers that are not yet discovered and, once they found them, they can be relayed as coins within the network. Miners are generating the wealth, then they put it in circulation at their own discretion.

Back in March 2011, still a few months before the popularization of Bitcoin which unavoidably raised the level of noise for the discussion about it, netizen Mira Luna blogged on his/her journal “Trust is the Only Currency” what I believe to be the best criticism elaborated upon Bitcoin. I’ll quote here the conclusion of this blog post, titled “BitCoin: a Rube-Goldberg machine for buying electricity”⁸:

In the end, the artificial creation of the limited number of possible BitCoins via this "proof of work" (doing millions of SHA-256 hashes over and over) is madness. All you really need is to have "proof of limitation" without the politics—was the market restrained from creating too much money too fast? BitCoin's use of a procedural solution is the wrong track when all you need do is define a constraint via a formula and apply it as needed over time, instead of everyone continuously spinning a hash function and wasting electricity. Keep the transactions public, cryptographically sign them, and audit them with a money model and you'll be able to keep much of what is good about BitCoin. And of course, use a "commodity" the people can intuitively understand, something like... time.

To go further this criticism we need to explain what this *madness* is and why it can be considered instead an interesting innovation. When miners do their work (hence consuming electricity) Bitcoins “magically” appear, but their work also benefits the community: they strenghten the network of trust by making bitcoins less likely to be counterfeited.

The computation of mining and hence the electricity, is to strenghten the authentication of Bitcoin. Now let us consider the energy that was required, before the existance of Bitcoin, to authenticate the minting process of currency made in paper and less noble metals. It consists of a secret minting procedure, big machinery, a monumental building with thick walls and armed guards on its perimeter: an unstable kind of energy, very difficult to govern, as it relates to a *monopoly on violence* imposed by the sovereign state.

This very energy is substituted by Bitcoin with a qualitatively different approach: Bitcoin distributes peers to the task of building *trust in its authenticity*. The networked computation of all miners serves as a mint and dissolves the need for violence into an unlimited, unreachable and decentralized power.

Clustering the mint gathers the energy necessary to establish and protect the authenticity of the currency.

In other words: participation has substituted violence in the physical implementation of currency authentication: a recognizable pattern when we observe historical manifestations of the digital plane of immanence.

This passages leaves still open the problem of redistribution for the minted coins: it does not solve the problem of shared wealth. But we are now back to a familiar problem for money, after having dispelled the risk of a paradoxical machine, the Rube-Goldberg, which would have dissolved the Bitcoin’s concept of work in pure entropy.

5.3 Accounting science

The most remarkable innovation brought by Bitcoin deals with the system of accounting that we use today. Double-entry bookkeeping is what we use today to make sure that earnings and expenditures match, basically authenticating the flow of money and making sure “nothing is duplicated”.

From an historical perspective, the double-entry bookkeeping system is very ancient and barely actualised through the ages: it was described by an Italian mathematician and Franciscan friar named Luca Pacioli in his book “Summa de arithmetica, geometria, proportioni et proportionalità” published in 1494 in Venice. The second

⁸Blog article on <http://trustcurrency.blogspot.nl/2011/03/bitcoin-rube-goldberg-machine-for.html>



Figure 2: Friar Luca Pacioli (portrait by Jacopo de' Barbari, 1495)

half of his book, dedicated to geometry, is a section titled “Trattato de computi e delle scritture” in which he describes the necessity of mathematics in accountancy. Those principles were certainly not invented by Pacioli, but mostly actualised, formalised and translated in his tractatus, as demonstrated by the existence of a previous book “Della mercatura e del mercante perfetto” by Benedikt Kotruljević published in Latin some decades before, or as hinted by the presence of another figure behind his portrait in the famous painting attributed to Jacopo de' Barbari (*Figure 2*) who is believed to be Albrecht Dürer, an artist and traveler who shared Pacioli's passion for geometry and magic.

Such a system is still, as of today and despite its flaws, the one in use on large scale around the world by most accountancy systems. Being a system that ensures the univoque matching of what is written with what is real, it can be seen as gateway to the digital dimension and can undoubtedly benefit from the technical innovation through digital tools. Hence my argument that Bitcoin is basically this innovation or, more precisely, the implementation of an innovation as the *triple-signed receipt* method. Quoting Ian Grigg:

The digitally signed receipt, with the entire authorisation for a transaction, represents a dramatic challenge to double entry bookkeeping at least at the conceptual level. The cryptographic invention of the digital signature gives powerful evidentiary force to the receipt, and in practice reduces the accounting problem to one of the receipt's presence or its absence. This problem is solved by sharing the

records - each of the agents has a good copy. In some strict sense of relational database theory, double entry book keeping is now redundant.⁹

The accounting system of triple-signed receipts in Bitcoin respects the original role of money as contract (and digitized speech, I'd argue). Quoting Marco Sacy's research on complementary and alternative currency:

The ontology of money is as relational, abstract and cogent as agreements are in general and the possibilities to formulate these agreements are unimaginable, bearing in mind that the orthodox process of currency design and creation is - drawing from Adorno and Horkheimer's Dialectic of the Enlightenment - an arbitrary and historically determined one.

It is the very substance of those *cogent agreements* that money represents and can be verified by matching declarations on two books or, as Bitcoin does, calling the whole network of participating peers to witness every contract and entangling it into a cryptographic blockchain. Simply put, this is bookkeeping in the age of Bitcoin.

6 Community

At the core... is the idea that people should design for themselves their own houses, streets and communities. This idea... comes simply from the observation that most of the wonderful places of the world were not made by architects but by the people.

Christopher Alexander

When talking about Bitcoin, of its inherent qualities of networked creation of value that were just mentioned, we can't ignore the fact that this technology relies on community dynamics to the point one could state that Bitcoin makes it possible for *money to become a common* and no longer a top-down convention imposed by a sovereign and its liturgy of power.

But then we are faced by a crucial question about Bitcoin: what for? who benefits from it? or, in other words, if the community aspect of Bitcoin is crucial (as in: distributing the computation needed for its authentication, sharing a common currency, a common history of transactions, a common way to quantify wealth) what do the communities use Bitcoin for?

The earliest communities that adopted Bitcoin, aside from the hacker community that never really used it much as a currency to exchange goods, are perfect scapegoats for those who want to turn Bitcoin down. In fact, anyone willing to take a moralistic approach and prohibit the innovation that we are talking about doesn't even need to approach itching concepts such as state sovereignty. It is very easy for witch-hunters to emphasize the fact that drugs were bought and sold with Bitcoins, that gamblers love Bitcoins and that some website claims to accept Bitcoin payments for assassination missions. Criminalizing campaigns have been overly present in the mainstream media coverage immediately following the popularization of Bitcoin, in Italy we've seen even popular prophets of Internet optimism turning against Bitcoin in the blink of an eye¹⁰.

But then, speaking about new technologies, we should never rush to judge their nature and goals from their early adoption. It is natural that those who were excluded from the use of established technologies will look for new as yet unregulated platforms: pioneers at the margins are always attentive about the concrete possibilities of liberation offered by new and unknown tech. When speaking of communication technologies this becomes very clear: all kinds of marginalized and criminalized communities resort to lesser known channels of communication for their needs, while mass communication channels are well policed and in general dominated by the sanitized discourse of the conformed majority. The motivation to debate what moves prohibitionists in their crusade is far from this article, yet what needs to be stated here is that the potential of new tech cannot be studied, understood and judged referring to such circumstances. The examples provided on the early adoption of Bitcoin are in fact misleading to obtain a balanced comprehension of this tech.

The fact is that many hackers love to tease and this attitude, united with a discrete amount of criminals that found it convenient to use Bitcoin since the early phases of its popularization, still offer grounds for the mystification of it as an "evil technology".

⁹Grigg, 2005 - http://iang.org/papers/triple_entry.html

¹⁰People like Riccardo Luna for instance, a televised advocate of Internet and digital innovation in Italy, started a media crusade against what he calls the "Dark web"

Being involved in the community that has grown around Bitcoin I can see that the community is comprised primarily of young idealists rebelling against the status-quo, especially when it consists of a centralized administration prone to corruption. It is clear to many how unjust monopolies are often dominating various contexts, curbing the possibilities of innovation that are in the hands of younger generations. The liberation of the medium of value exchange is an act we refer to as “breaking the Taboo on Money”. Bitcoin has a role in history: its epos coalesces in communities, new ethical reflections, new tales of passion, the glory in all the mystery around its origins. The will for liberation, decentralization and disintermediation is central to Bitcoin - it is ethical and should not be seen as more conflictual than the concrete need to disintermediate many of the systemic functions that are governing modern society. Mind your own long-tailed problems, modern finance!

Many see in Bitcoin the opportunity to challenge the bank monopoly on value transactions. Most goods that were first exchanged on-line for Bitcoins, beyond the dark waters, digital or not, are artisanal creations. The Bitcoin dream is the autonomy of content producers, to exchange their production freely, without aggregations, without intermediaries. After all, most financial transaction operators know well that the reason that small artisans cannot enter on-line markets are the high marginal costs they need to face if they want to accept on-line payments, while the apparata that are able to negotiate trust with banks are imposing themselves as taxing intermediaries.

As a concrete yet slanted hint to the reader, he is my little protest against the **capitalism of flows**, an informal text that I’ve posted on the Nettime discussion list back in April 2011, slightly before the popularization of Bitcoin in the Forbes article published in May. While responding to early criticism of Bitcoin, this letter ended up being circulated on the Bitcoin forum and as the “Bitcoin Manifesto”, gathering approval from different members of the community¹¹:

On Thu, 07 Apr 2011, a . . . @aharonic.net wrote:

> bitcoins - isn't this simply a distributed structure to do capitalism with?

That's not even the worst you can do with it. you can do money laundering, buy drugs online and sex toys, all anonymously. but that's not the point, because despite the coercion imposed by all kinds of regulatory systems so far, also current official monetary systems are full of that shit, on top of the capitalist pie.

Emerging technologies should never be judged by the sensationally bad taste of early adopters. it's like being concerned about the shit that fertilizes some beautiful flowers, wasting their seeds.

What bitcoin really is, I finally understood on the 6 april (which somehow always ends up being a magic day, eh!): this is now the end of the **flow capitalism**, which consists of the monopoly on transactions, the hegemony of banks on the movement of values and not just their storage, this middle-man mafia strangling the world as we speak.

How right are those South American countries asking for the “taxation of transactions”, an argument refrained in many speeches of the *compañeros*. They studied the system and understood that there is a crucial problem, that needs to be solved urgently. Yet I'd argue that taxation on transactions cannot be the solution. The solution is to eliminate the flow capitalists.

If I want to give you money I'll give it to you. Me and you, period. Its fine that we'll pay our taxes for our communities, don't get me wrong this is not a tea bagger argument. Its just not right that all what we do is in the hands of a third party that has already been caught cheating many times: look at what happened at the Paypal accounts of the Iraqi Linux user group back in 2004, or even more recently to Wikileaks.

We don't need those fat cheaters to be in between our value transactions anymore; the flow capital has played its disgusting role in the little laps of history for which it has been needed, now sadly these people won't give up what they have accumulated, so it makes more sense to leave them alone and multiply more monetary systems that work efficiently across diverse networks and that rely on the neutrality of a cryptographic authentication.

The death of the flow capital is a new stage for the necrotization of capitalism.

¹¹Bitcoin forum thread “Bitcoin Manifesto” on <https://bitcointalk.org/index.php?topic=5671.0>

Beyond the shouted points made in this little speech lies an important hint: *Bitcoin will be of central importance for migrant economies.*

Today it is easy to witness the existence of large communities that are displaced around the world in the desperate attempt to recuperate over the territorial differential of value for their labour. Many of those who work abroad are sending money back to their families and communicating constantly with them, a natural phenomenon by which the market of telephone and money transfer shops all over the world flourish. These nodes of communication are extremely important for migrants, who can't live without them and most of the time end up being harshly taxed for their use. Monopolies like that of Moneygram or Western Union claim that no commission is applied to transactions, but their de-facto currency rates sometimes hide up to 20% for their profit.

Such profit on transactions is made upon data transfer that is comparable to that of a telephone call and it is not a coincidence that such shops often offer both services. Today there is no reason why such market of digital transaction shouldn't be freed in a fashion similar to what Voice over IP did for telephone monopolies. This is an old vector of evolution offered by the digital dimension and its progressive interaction with reality, that I call *digital immanence*: yet another scheme based on the artificial economy of scarcity is trembling!

7 Passion

Previously I've mentioned that Bitcoin's epos coalesces in new tales of passion.

For every process of subjectivity emerging in history, passion is crucial. Analyses such as the one conducted by Giorgio Agamben in his enquiry on sovereignty and glory show that it was historically possible to codify passion (and its mysteries) into power. Through the analysis of the ancient codes constituting laws and ethics (while also celebrating the glory of angels), Agamben shows that the power (and mystery) of passion is close to that of economy and its birth.

```

---BEGIN TRIBUTE---
#./BitLen
::::::::::::::::::
::::::::::::::::::
:::.'''':
:::''',xiW,"4x, ''
: ,dWWWXXXXi,4WX,
' dWWWXXX7" 'X,
  lWWWXX7  _ _ X
:WWWXX7 ,xXX7' "^X
lWWWX7, _.+,, _.+.,
:WWW7,.'^-"' ^-'
WW",X: X,
"7^Xl.  _(_x7'
l (:X:  _ _
'. " XX ,xxWWWXX7
)X- "" 4X" .___
,W X :Xi _,-
WW X 4XiyXWWXd
"" ,, 4XWWWXX
, R7X, ""447^
R, "4RXk, _ ,
TWk "4RXXi, X',x
lTWk, "4RRR7' 4 XH
:lWWWk, ^" '4
::TTXWwi,_ Xl1 :..
=====
LEN "rabbi" SASSAMA
1980-2011

```

```

Len was our friend.
A brilliant mind,
a kind soul, and
a devious schemer;
husband to Meredith
brother to Calvin,
son to Jim and
Dana Hartshorn,
coauthor and
cofounder and
Shmoo and so much
more. We dedicate
this silly hack to
Len, who would have
found it absolutely
hilarious.
--Dan Kaminsky,
Travis Goodspeed

```

```

P.S. My apologies,
BitCoin people. He
also would have
LOL'd at BitCoin's
new dependency upon
ASCII BERNANKE
::::::::::::::::::
:::.'''':
::: _.' _.' _.' :
: _,' ^" " ^x, :
' x7' '4,
XX7 4XX
XX XX
Xl ,xxx, ,xxx,XX
( ' _,+o, | ,o+,"
4 "-^' X "-^" 7
l, ( )) ,X
:Xx,_ ,xXXXxx,_ ,XX
4XXiX'-___-'XXXX'
4XXi,_ _iXX7'
, '4XXXXXXXXXX^ _ ,
Xx, ""^^^XX7,xX
W,"4WWx,_ _ ,XxWWX7'
Xwi, "4WW7""4WW7',W
TXXWw, ^7 Xk 47 ,WH
:TXXWw,_ ), ,wWT:
::TTXXWWW lXl WWT:
----END TRIBUTE----

```

Figure 3. Extract from a very early chunk of Bitcoin’s main blockchain

Figure 3 shows an ASCII extract from the Bitcoin blockchain, a tribute that was irremediably inscribed in the transaction history chain. A memorial to a leader of the “cypherpunk movement” is codified, literally, into Bitcoin’s “blockchain”, decorated with typical hacker irony. This is just a hint of what may appear as an “insider joke”, but is in fact the strong trace of a shared narrative.

The historical episode of passion in Bitcoin is connected to another project that is strictly related to the cypherpunk movement: its name, incredibly well known today, is Wikileaks.

Wikileaks has provided the supreme moment (καρπός) for Bitcoin to become an urgency within the cypherpunk imagination and that of hackers at large: I’m talking about the financial blockade to Wikileaks.

Below is an excerpt of the account that Wikileaks staff makes of this episode on their website, to which is dedicated a whole page:

Since 7th December 2010 an arbitrary and unlawful financial blockade has been imposed by Bank of America, VISA, MasterCard, PayPal and Western Union. The attack has destroyed 95% of our revenue. [...] The blockade is outside of any accountable, public process. It is without democratic oversight or transparency. The US government itself found that there were no lawful grounds to add WikiLeaks to a US financial blockade. [...] The UN High Commissioner for Human Rights has openly criticized the financial blockade against WikiLeaks. [...] The blockade erects a wall between us and our supporters, preventing them from affiliating with and defending the cause of their choice. It violates the competition laws and trade practice legislation of numerous states. It arbitrarily singles out an organization that has

not committed any illegal act in any country and cuts it off from its financial lifeline in every country.
[...]

In the US, our publishing is protected by the First Amendment, as has been repeatedly demonstrated by a wide variety of respected legal experts on the US Constitution. In January 2011 the U.S. Secretary of the Treasury, Timothy C. Geithner, announced that there were no grounds to blacklist WikiLeaks. There are no judgements, or even charges, against WikiLeaks or its staff anywhere in the world.

The blockade was an immediate reaction to the “cablegates” release, where an enormous amount of classified USA diplomatic documents had been published by Wikileaks. This episode did not please many powerful people in USA (arguably, Wikileaks has hit its military-industrial complex in many ways). Though the Wikileaks organization received much appreciation from all over the world, also in the form of monetary donations. While the media wave of cablegates was reverberating through the world’s screens, international transaction monopolies like Maestro and Visa blocked Wikileaks from receiving donations, without a legal mandate, nor a courtcase order. Wikileaks also had its registered Internet domains obscured, with the exception of the one registered in Switzerland.

Hackers believe the world can be changed and, while understanding the importance for code and shared protocols, they are determined to play on *neutral* grounds, which is also a condition for change to happen. Some readers may judge hackers as naïve for believing that there can actually be *network neutrality*, most system analysts, even in the financial sector, have recognised the presence of long-tail errors. Those familiar with the principles enunciated in Taleb’s Black-Swan will agree that it is impossible to establish neutrality within a tainted system, but, for the hacker community at large, the Wikileaks financial blockade was a radically new moment of fundamental betrayal. Thus it was a crucial momentum for the growth of Bitcoin: several hackers adopted it right in those days, feeling it was, rationally, liberally, the next thing to do. The growth of Bitcoin started then, as visible in *Figure 1* it was 5 months previous to the first Forbes article that popularized it.

8 Glory

Glory, in theology as much as in politics, is what takes the place of the inconceivable void that is the idleness of power; nevertheless, is this very inconceivable emptiness that nourishes and feeds the power (or, better said, what the apparatus of power transforms in nourishment) Giorgio Agamben

Every form of currency, since the very beginning of its earliest forms, has dealt with the grammar of power. It is the establishment of a sovereign and its glory that justifies the shared trust into a symbolic form of value circulation. The investment of power into currency, especially when its not backed by mineral values, is codified in mystery and glory.

Bitcoin is not exempted from such dynamics: it innovates the way the digital becomes tangible, a role with highly disruptive potential. Hence, even when choosing the iconography for its own currency, the Bitcoin community shows a political rupture.

The intriguing mystery of the identity of its disappearing author Satoshi Nakamoto, might seem a detail, but not for our analysis: it is of central importance to the Bitcoin myth and that of future crypto-currencies. Bitcoin has no single monetary authority, but a shared pact and the underlying rationality of a mathematical algorithm - the intangible dream of neutrality. Being deflationary, Bitcoins exist within a finite range of possibilities, a quantity of value that is increasingly difficult to mine. No one can create more Bitcoins than those established to be created in the first place, to the great horror of modern economists that regard fiat currency as a necessary tool to move within the troubled waters of contemporaneity, with good reason indeed. But there is no hierarchy in Bitcoin: meaning literally that there is no sacred origin (ἱεραρχία), no written fate, no single ruler, no second thought on its essence.

Bitcoin promises to be the neutral medium for an economy based on participation, not the edict of a king, a central bank, or their authorized intermediaries - nevertheless, it must be said, Bitcoin did create new riches, those who believed earlier than others in the promise of this algorithm. The rupture offered by this new perspective on money is not dealing with equality or welfare, it might not benefit society or help us get out of the crisis: it is a protest for network neutrality.

Such a medium, we must also admit, will likely incarnate the market freedom of the Austrian school of economics. The European Central Bank has produced an analysis of the Bitcoin scheme in October 2012 reciting:

The theoretical roots of Bitcoin can be found in the Austrian school of economics and its criticism of the current fiat money system and interventions undertaken by governments and other agencies, which, in their view, result in exacerbated business cycles and massive inflation.

This insight should be handled carefully: it might overstate on the ambitions of Bitcoin, which first and foremost is a successful implementation of a system for value transactions in the digital domain, whose success is due to the biopolitical dynamics we are exploring in this article. Nevertheless, the interpretation of its ethos in fieri is not far from reality. It is paradoxical how, in a time in which we face the failure of most Austrian economic theories, we are confronted with narratives that mystify and popularize them on the wave of technical innovation and functional transformation. But this is a reductionist way to describe Bitcoin and it strictly depends from the adoption of universal categories: I am convinced such a method of analysis can't lead the quest for comprehension we are engaging here. So let's take a step back from this dead end and look into Bitcoin's symbology.

If we look back in the history of icons used to mint money, we'll find a long stream of symbols of leadership: heads or bodies of humans or animals that address or signify the power of scientists, rulers, educators, judges or that of a nation-state. Many are the symbols of hierarchy that govern the minting and authentication of the currency, as well symbols of wealth and geographical maps. I'll refrain now from engaging an analysis of such symbols used in the past, but observe that Bitcoin has and will have a different symbology to glorify it.

The iconography of Bitcoin reflects the shared values of the community behind it. If there would be a person representative of it, this would be its mysterious creator Satoshi Nakamoto, but the fact that he doesn't really exist makes things much more interesting. One of the early symbols of Bitcoin was alpaca, for instance the mockup presented here comes from an old forum's thread and in its own way it is meant to celebrate the first artisans that ever sold their creations on the Bitcoin market.

As an experiment, in a previous article for the Bitcoin community I've suggested the use of the empty throne as a bridge symbol across classical, modern and post-human iconography. The image of an empty prepared throne (ἐτοιμασία τοῦ θρόνου) is an icon found in the Old Testament and in books comprising the Upanishad, a sacred icon whose value ".is never so powerful as when the throne is empty", commented once archaeologist Charles Picard. The empty throne was used on minted currency in the Augustan era and sculpted exemplars of it are found in Knossos and Rome.

But the response of the Bitcoin community to such an old symbol of power, despite the fact it could represent the absence of Satoshi Nakamoto, has been negative. Someone commented that "perhaps a broken empty throne would be even better, symbolizing the breaking of the old power", someone else suggested that "a physical Bitcoin should have a mirror in the middle. Bitcoin is all about the individual" and again another suggestion "Bitcoin is mercurial – it's quicksilver. It's the fool of the tarot and a touchstone. It turns base electrons into gold. It subverts and debases all norms and conventions. The fool is the perfect symbol for bitcoin". Many also acclaimed the use of the Guy Fawkes mask, already adopted by Anonymous, from the V for Vendetta comics and movie.

The glory behind Bitcoin is mostly shrouded in mystery, revolt against tyrannical injustice, the reclamation of individual rights, power distribution and the disintermediation and self-determination. But also, I strongly argue, by the transverse presence of a community feeling and the joyous consciousness that a powerful process is unfolding in history: those participating have the possibility to express themselves in their diversity, rather than the uniformed, sterile and omnipresent corporate language of economics.

After the phase in which the Multitude has built its body inside the language, the next opening cycle of conflicts will see the Multitude engaged in the construction of its body beyond language. Christian Marazzi



Figure 3



Figure 4: Protestors weaving a Bitcoin banner in Occupy Amsterdam, July 2012

9 Popularity

By now should be clear that such a process of subjectivation as the one we are describing is not the simple emergence of a new innovative technology, it is not just a *λόγος* on *τέχνη*, it goes well beyond. The enormous popularization of Bitcoin is proof that the dimensions of this process of subjectivation are multiple and cannot be comprehended by adopting a single narrative, and even less so by using the categories of economic analysis.

The popularity of Bitcoin as of today is enormous and still growing: this is a result of the biopolitical progression described above and its inscription inside a particular context, it is not a quality of Bitcoin alone. Bitcoin is rooted in the protest movements that accompanied the financial crisis through 2009 until now, namely the Occupy movement. While there can be reason to conceal this fact for those who hail the unconditioned and instrumental success of Bitcoin, it is important to account this historically in order to understand what might happen in the future.

The cultural scene around Bitcoin is shaped around new values that, despite their many pitfalls, incarnate the rebellion against “The System”. In the last Bitcoin conference in Europe we have clearly seen that those people closest to it are definitely interested in the larger picture: they are conscious that a systemic critique is the underpinning of Bitcoin existence, to the point that the next conference title changed from being focused simply on Bitcoin to being called the “unSystem” conference with among the speakers Anonymous, Occupy London, Voïna¹² and Birgitta Jónsdóttir¹³.

Being popular also means to be branched, forked, replicated, cloned, recombined and ultimately appropriated

¹²a Russian street-art group well known for their provocative and politically charged works of performance art.

¹³Member of the Constitutional Assembly of the Icelandic Parliament and former member of Wikileaks.

by the people: a popular icon will feed the mind of popular culture without consuming itself, but confusing its authenticity in the existence of new popular instances. This is already happening to Bitcoin with very interesting consequences. Considering that its popularity is mostly among the hacker (or, should we say, young cyborgs?) community, the branching of Bitcoin is giving birth to many valid technical implementations, that are both capable of functioning on large scale, and explore novel approaches to currency and networking.

Among the first forks of Bitcoin were ironic implementations of it: like Cosby coin featuring the popular TV star Bill Cosby with a computer, or Carrots - just carrots, or Weed which was a currency matched to the value of its developer's favourite Thai beer.

But there are also serious forks of Bitcoin, both alternative or complementary to it, and we can expect more in future: NameCoin (whose functionality is to register new network domains) or Litecoin (which can be mined on the same machines mining Bitcoins, without interference) are just some valid examples.

A particularly interesting one is Freicoins¹⁴ which grafts on ideas by Silvio Gesell for a monetary system with zero interest on credit: the value of currency "decays", meaning that as time goes by it loses value. Freicoins cannot work as the storage of value, a common practice among Bitcoin users, therefore it circulates faster. By implementing this feature, referred to as "demurrage", this is one of the most promising forks of Bitcoin today, at least in theory.

With my own pet project in the Bitcoin galaxy, something called Freecoin¹⁵, I've started documenting the phenomenon of forking Bitcoin since its early days and advocated within the community for the "configurability of the genesis code" and in general to leverage the possibilities of customisation for the technology underlying Bitcoin. It is my belief that, while Bitcoin represents a unique political rupture with the old establishment governing money, it is not the ultimate solution to it.

The need for digital currencies based on triple-signed receipts cannot be simply satisfied by Bitcoin. Nevertheless, strengthened by the popularity and all consequences we have explored here, Bitcoin might stand on the longer term as a fixed reference for future implementations: it is realistic to predict that its value will only grow in future.

10 Conclusion

The time has come to explain the title of this article, namely, that Bitcoin is breaking the Taboo on Money. For many years we have taken money for granted, without even questioning its engineering, without analysing accountancy in systemic terms. We have used it and we have been used by it. To paraphrase Georg Simmel, we have made ourselves "indirect beings", the intermediaries between money and the creation and satisfaction of our own desires.

Just like a taboo that is so close to us to make us turn the other way, we have avoided questioning what makes money exist. In the past 50 and more years people have quietly accepted the transformation of money into something more abstract, far from everyone's hands, in fact becoming just a number in the databases of banks, a gesture of interaction with computers that know more than we do about our possessions. While being the "root of all evil" for some, it has become close to a religion for others, but in both cases money has been too important to be questioned and its evolution too natural to be interfered with by the masses. It is a system that permeates most if not all societal interactions, at least in the Western world, so we assume it to be neutral and, in any cases, we will never question its existence.

Most political analyses study the dynamics related to the distribution of money, its relation to labour, accumulation, use value and exchange values. Universals have governed the entire discourse around monetary engineering

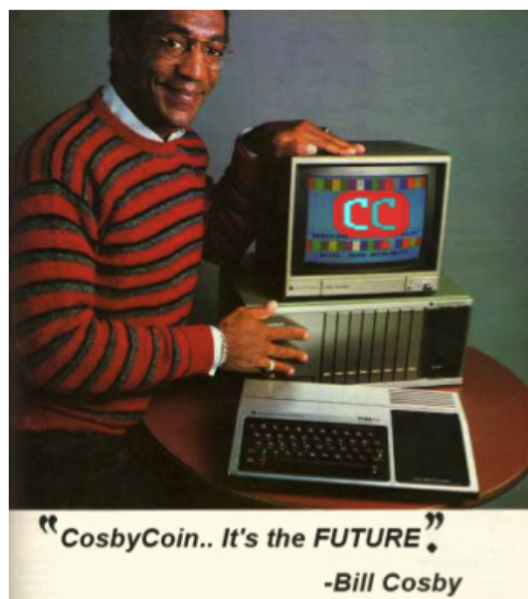


Figure 5: an ironical example of Bitcoin fork

¹⁴"Freicoins: a peer-to-peer digital currency delivering freedom from usury" <http://freico.in>

¹⁵"Freecoin is not a currency, but a suite to create P2P currencies" <http://freecoin.ch>

and mathematical models have been the method to explain its aspects. As a glaring exception to this, there are sociological analyses such as that made by Max Weber that evaluated the relationship between ethics and money across historical mutations of society. Yet, to this day, only few dared to look closer into currency systems and their biopolitical implications, without wearing the protective goggles of historically established universals: this has been a self-imposed taboo for many researchers and practitioners, to dissect this medium, just like a dead body that we are not allowed to study.

Now that money seems to be either dead or dying, it is the time to dare this dissection. It might be the case that, by trespassing this taboo, we will find out ways to change things on a larger scale, especially considering the long due line of innovation in the field of accountancy that has still to be applied.

Ultimately, there are proofs to the rupture I'm pointing out here, in the wake of many new currencies born after Bitcoin: with all irony and irreverence intended. The gates were left open by the mystery man: Satoshi the fool, Satoshi the saint, trespassed the line in front of everyone. There is no longer a taboo on money. Bitcoin is not really about the loss of power of a few governments, but about the possibility for many more people to experiment with the building of new constituencies.

11 Contributor details

Denis Roio, also known by his hacker nickname Jaromil, is an artist, activist and software developer at Dyne.org. His creations are recommended by the FSF and redistributed by several GNU/Linux and BSD operating systems worldwide, while he is also an active contributor to media theory discourses. Jaromil publishes conceptual art in digital form since the year 2000, has lead R&D activities in the Netherlands Media Art Institute for 6 years, was honored with the Vilém Flusser Award in 2009 and awarded a fellowship in the 40 under 40 program for young European leaders in 2012. He is currently writing his Ph.D. as candidate of the Planetary Collegium M-Node at NABA in Milano.



Figure 6: Portrait courtesy of Robert Lloyd

12 References

- Simmel, G., 1900, “Philosophie des Geldes”, DigBib.org
- Foucault, M., 1979, “Cours au Collège de France 1978-1979”, Feltrinelli
- Levy, S., 1994, “E-Money”, Wired USA, issue 2.12
- Lietaer, B., 2001, “The Future of Money”, Random House
- Flusser, V., 2002, “Writings”, Minnesota Univ. press
- Marazzi, C., et al., 2003, “La Moneta nell Impero”, Ombre Corte
- Ascott, R., 2003, “Telematic Embrace”, Univ. California press
- Grigg, I., 2005, “Triple Entry Accounting”, Systemics Inc.
- Agamben, G., 2007, “Il Regno e La Gloria”, Neri Pozza
- Nakamoto, S., 2009, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Bitcoin website
- Negri and Hardt, 2010, “Commonwealth”, Harvard Univ. press
- E.C.B, 2012, “Virtual Currency Schemes”, European Central Bank
- Sachy, M., 2012, “The empowering potential of complementary currencies and alternative payment systems”, Silent University Tate Modern