Myth, machinery and cryptocoin avarice

Haraši Namztohoto[1]
harasi@teracoin.org

Abstract

Cryptocoins are peer-to-peer monetary assets emitted not by a central authority but by a decentralised network of economy's participants. Their existing implementations combine the state of the art cryptographic methods with notions of « transparency of coin's history » and « pseudonymity of usage ». While the market value of Bitcoin -which was the first among the cryptocoins - is very volatile, it nonetheless becomes more and more demanded an asset due to its a priori defined limited amount. Thus, a billion dollar economy has already formed in the cryptosphere, which includes the stock markets, currency exchange offices or a biggest existing online drug market. By this paper we aim to address the questions like « To whom do the structures like Bitcoin ultimately serve ? » and to propose an idea that further growth of cryptocoin economy could induce a sort of Nietzche's «transvaluation of values».

Keywords : bitcoin, cryptography, pseudonymity, transparency of history, hoarding, trading addiction, cryptocoin operation generator, peer-to-peer, planetary AI emergence

1 Hermeneutic reference

In a novel which has, since less than 20 years from its publication (Stephenson, 2003), already became a classic of post cyber-punk litterature, the main story's character – a somewhat subversive nanotech artifex named John Percival Hackworth – concieves a device aiming to attain sufficient amount of computational power neccessary to compute the molecular structure for the entity called « The Seed » (Drexler & Minsky, 1990). The aim is attained by a peer-to-peer network of replicable computational agents inducing the human hosts within which they are embedded, to execute the ultimate act of computation by means of exchange of bodily fluids.

In our reality, however, there is no Hackworth and the idea of Artificial Intelligence being active also on the nanoscale is yet to be realised. But since a group of peer-to-peer decentralised computational devices is being more and more deployed on a planetary scale, and since these devices – which we shall label as « cryptocoin operation generator » (COG) in the rest of this paper - serve as a vector maybe not for sexual intercourse, but for a more common exchange of goods&services; and since it may be the case that Stephenson's preceding book, Cryptonomicon (Stephenson, 2000), containing dialogues like :

"What's an electronic banknote look like, Randy?"
"Like any other digital thing: a bunch of bits."
"doesn't that make it kind of easy to counterfeit?"
"Not if you have good crypto," Randy says. "Which we do."

could have possibly inspired Satoshi Nakamoto to publish the first version of his Bitcoin client as well as the academic article (Nakamoto, 2008b) describing the intricacies of its function, we found it neccessary to start our excursion into the world of cryptocoins with the references hereby proposed.

2 Satoshi myth

« There once lived a man, or a group of wayfaring men (Rosenberg, 2007) , who have chosen the token Satoshi Nakamoto for their name. And bitcoin's code they programmed and to other men that code they gave. »

With such words could possibly begin the « myth of Satoshi » if ever the Bitcoin's author decides to stay anonymous, as he has done until now. It sounds strange but it is true – with exception of the author (him|her)self, nobody knows which brilliant mind have opened the Pandora's box. The only thing certain is that, between 2nd November 2008 and 25th January 2009, eighteen messages were sent from the user Satoshi Nakamoto to mailing list cryptography@metzdowd.com and in the same time, a domain bitcoin.org was established linking to corresponding source code repository at sourceforge.

While everything else concerning the persona itself is more and more opaque with time, the motivation behind the project's deployment was clearly libertarian, as is evident from Satoshi's reply to objection that « [one] will not find a solution to political problems in cryptography » :

« Yes, but we can win a major battle in the arms race and gain a new territory of freedom for several years. » (Nakamoto, 2008a)

Thus, it seems that the ultimate motivation of Bitcoin deployment was a kind-of Prometheic impulse to liberate mankind from ever-strenghtening state which is often being percieved as a yoke of bank-governed reality. In combination with Satoshi's anonymity, the story has all the prerequisites to become *une narrative par excellence* for disenchanted post-modern global world. By revealing his identity, Satoshi has good chances to obtain a Nobel prize and obtain a high-listed in place in Forbes ever-growing list. But by conceiling it, his deed could become as mythical as those of Achilles.

3 Transparency but pseudonymity

One of Satoshi's most innovative ideas was to couple the process of distribution of new coins – or « coin min(t)ing » as it is often called – with the process of transaction authorisation. A cryptocoin, in its very essence, is nothing else than a chain of digital signatures -from the « coinbase » origin to current owner - generated by means of Eliptic Curve Digital Signature Algorithm (Lopez & Dahab, 2000). Every signature in itself is essentially the information about address of an account to whom the amount was transferred with the information about the quantity transferred, signed by the private key of quantity's owner[1]. Given the fact that cryptocoins are, in the end, just pure information, a robust transaction authorisation mechanism is of crucial importance for a system of exchange of such assets. Most importantly, it has to be assured that no « double spending » takes place, i.e. that the coin C which a user U has in the moment M cannot be used twice in the moment M+1 and/or M+2. Nakamoto's elegant solution to the problem was to 1) multicast the information about the transaction to sufficient number of nodes of the network 2) to use a computationally expensive procedure, a SHA-2 256 hash (Gilbert & Handschuh, 2004) reversion problem as a « proof-of-work » mechanism whose principal objective is to minimize the possibility that some node in the network shall succeed to overwrite the transaction history (called « blockchain ») in a so-called « >50% attack ».

This being said, we precise that it is not intention of this article to explain the intricacies of the Bitcoin algorithm since this was already done thousands of times with bigger or lesser success. But what we consider it important to focus reader's attention upon the fact that in the world of cryptocoins, the trajectory of coin – from the very moment since it was « min(t)ed » by one among

1 In reality, the whole thing is somewhat more intricate, and what is being signed is, in fact, a script in a scripting language more complex than simple « transfer quantity from A to B » instruction.

multitudes of network's COGs, until its curent owner – is broadcasted to all nodes of the network and thus completely transparent. We call this feature of cryptocoin monetary assets « **transparency of history** ». Anyone running a bitcoin server or any visitor of sites like blockchain.info can, with sufficient patience, observe the trajectory of every single coin, from the « coinbase » to current owner's address. But since it is quite easy for any user to generate multitudes of account addresses – which are nothin else than publicly broadcasted cryptographic keys which cannot be actively used without knowledge of a « private key » from which they are generated during the account address creation process and which only the owner knows – it is very difficult, if not practically impossible, to create a link between a cryptocoin address and a physical entity holding the key to that address if that entity herself does not want to reveal her identity. While the lack of this bridge between the virtual and the real which we call « **pseudonymity of use** », is applauded by advocated of libertarian cryptopunk movement as a highly welcomed and positive feature, it brings itself a growing concern that, in the long term, such a complete opaqueness shall, above all, be profitable especially to those who conduce financial activities which they would normally hide.

3 Min(t)ing and trading

In simple terms, there are only two ways how Bitcoins, or other cryptocoins – with exception of PPcoin- can be earned: by mining and by trading. Miners are those who invest the computational power of their ressources into verification of validity of transaction broadcasted within the network. Since the probability of discovery new block of coins is proportional to the amount of computational ressources invested into the mining, it follows that the biggest number of new « virgin » coins will become the property of those who invested biggest amount of computational ressources. It seems that first few months of Bitcoin existence, the algorithm was running only on CPU of Satoshi Nakamoto where he had possibly pre-mined cca 1 million bitcoins (Bitslog, 2013), subsequently other CPUs joined the network, then a much faster SHA-2 hashing performance was made possible by exploiting the faculties of graphic card's GPU. With market value of bitcoin gradually rising, the hound race continued with deployment of first Field-programmable gate array (FPGA) bitcoin mining devices in order to continue with cohorts of Application Specific Integrated Circuits (ASIC) spouted from factory's conveyor belts somewhere in Pudong economic zone. Given the fact that these devices can be bought, in the first place, for bitcoins, the whole bitcoin economy started to ressemble an initially purely virtual but with time ever-more-real Uroboros snake reiyfing itself by the processus of software being materialized in hardware, and as may be the case in days to come, also into wetware of organic tissue.

Initially, only informatic-oriented services were tradable for bitcoins and only very rarely were some more material transactions executed - as was the case, for example, of the most expensive pizza[2] of mankind's history. Later some coffee producers and Alpaca-socks distributors joined the club but the things changed with the launch of « Silk Road », an online drug marketplace (Barratt, 2012). By harnessing the anonymising possibilities furnished by a « TOR hidden services » protocol (Dingledine, 2005) and combining them with pseudonymity of Bitcoin's financial transactions and a simple escrow service business model, SR's developpers succeeded quite fast to transform their supply-demand coupling e-bay like bazaar website, possibly running somewhere on a server in grandma's backyard, into a multimillion enterprise .

In parallel to SR, online exchange offices like Vircurex or Mtgox started to flourish where it was possible to trade BTC for real-life fiat currencies. Whole stockmarkets emerged, making it possible to

2 Traded for 10000 BTC in 2010. 3 years later, an estimated market value of the such an amount of BTC would be more than 1 million US dollars

find investors for one's project. Gambling and betting industry swiftly followed with projects like Satoshi Dice adding another level of anonymity to already opaque activities taking place within the cryptosphere. Being an ideal haven for money-laundering and tax-evasion, Bitcoin economy gets mundane and flourishes.

4 Algorithmic quasi-deity

As of 2013, Bitcoin has all prerequisities to become a new religion for the world where « death of god » (Nietzsche, 1911) is a widely accepted truth. It has its myth of creation and the living testament of those who had eaten a million dollar pizza. It has its disciples – mostly computer geeks who became millionares because they were connected to right discussion forum or Internet Relay Chat (IRC) channel in the right moment. And it has its devotees – people who invested their fortune and hundreds of hours of their lifes in exchange for the hope that the Bitcoin economy shall turn out to be something more than a pyramid game ; often people who know that in order not to lose what they had invested, they had to spread « the bitcoin gospel ». It has its more and more omnipresent « giving deity » - a consensual algorithm based upon a simple inflationary curve which distributes according to the promise that the biggest amount of « virgin » coins shall be given to those who invest the most into keeping the whole machinery going – the whole processs being probabilistic, thus containing neccessary amount of hopeful waiting sometimes crowned with blissful surprise. And at last but not least, the BTC monotheism syndrome has its old idols to overthrow, idols like Ayn Rand's dollar (Rand, 1957) which paved the way but lost their power as gold once lost it, *mutatis mutandi*, when gold standard was abolished.

Given these propositions suggesting that bitcoin mania can involve not only frontal cortex, but also amygdala or even pineal gland (Paloutzian & Park, 2005), it is of no surprise that even reasonable people consider as not only possible but even plausible the state of things whereby the information concerning the transaction of two potatoes in Ushuaya is broadcasted to millions node of the cryptosphere, Papua New-Guinea included. Reason often discretely quits the cognitive battlefield whenever hoarding (Mataix-Cols et al., 2010) tendencies of human beings are coupled with addictive behaviour which financial derivate trading surely is, thus leaving humans prone to caprices of mass psychology. And as of spring 2013, slowly resurrecting from the implosion of the second deflationary bubble when the market value felt from 260 USD to 80 USD in one day, Bitcoin is again gaining momentum and becoming truly massive.

5 Clash of the Titans

Contrary to an ancient greek coin lying forgotten in the dust which guards its value *by simply being an object it was created to be*, Bitcoin need to burn energy in order to survive. What's more, the minting hound race obliges any minter to burn still more-and-more energy in order to keep pace with other minters. When one takes into account all the machinery dedicated to making the network run + the machinery which makes the machinery which makes the network run, one is obliged to admit that Satoshi designed a monteray system addressing social and political issues but ignored the ecological ones. More precisely – given the fact that without ever-growing energy consumption caused by min(t)ers, the transaction blockchain could be overwritten by the node obtaining more than 50% hashrate of the network, the whole machinery cannot be stopped or even slowed down because if slowed down, it will cease to be a secure value-carrying haven. Thus, the Bitcoin architecture has to lead, *ex vi termini*, to the scenario « Tragedy of Commons » (Garrett, 1968) scenario.

Luckily enough, some people have already understood that Nakamoto's Bitcoin was nothing else than a prototype and that the values of parameters determining the overall functioning of the network were just one set of values among multitudes of other, possibly more optimal values. Thus, after a first wave of alternative cryptocoins like SolidCoin, LiquidCoin, IxCoin, I0coin or FeatherCoin whose objective was no else than to make those who deployed them rich, and which have not brought any substantial adjustment to Nakamoto's original code, a second wave of alternative cryptocoins like TerraCoin, LiteCoin or PPCoin are gaining momentum, each bringing with itself at least one novel feature. PPCoin (King & Nadal, 2012) seems to be of particular interest due to the importance its author put upon long-term ecological sustainibility as well as due to the fact that it is the only cryptocoin which is not purely deflational but integrates a very gentle inflation into the model. TerraCoin is of interest due to differences values of the network's intialisation parameters and LiteCoin – currently the second strongest cryptocoin – attracts more and more attention because its proof-of-work component is based on the scrypt algorithm (Percival, 2009). Since the scrypt algorithm involves not only simple hashing but demands the participation of huge amounts of memory, it is much more difficult to execute it on specialised FPGA and ASIC hardware, thus making LiteCoin more attractive for min(t)ers disposing only of classical computers.

Due to the growth of the cryptocoin diversity it is therefore far from certain that the cryptosphere shall, in the years to come, venerate by its activity only the Ƀ divinity. One can only hope that sooner or later a cryptocoin shall be proposed which will harness the computational ressources of the COG devices involved for some noble a task – be it anticancer protein modeling, climate prediction or astrophysical data analysis. But until global deployment of such cryptocoin shall take place, all other cryptocoins shall principally address nothing else than hoarding tendencies common to a superior primates which a *homo sapiens sapiens* undoubtably is.

6 *Umwertung aller Werte*

By pure coincidence did the author of this article bought, in February, 230 Terracoins for approximately 1.4$. Two months and two mouse-clicks later, the amount could be easily tradable for more than 140$ on vircurex exchange, net gain thus being approximately equivalent to 4 monthly wages of a full-time worker in garment industry in Bangladesh. Putting aside the possible trading addiction (Taleb, 2005) which could emerge if ever such behaviour-conditioning rewarding experience shall be repeated, one is obliged to pose the question: „What purpose do the cryptocoins truly serve and what value do they have ?"

And what value does a LiteCoin have, if in the same moment, in the same market place, one can buy it either for 4 dollars or 0.02 Bitcoins, given the fact that in the very same moment, in the same market place, one can buy a Bitcoin for 100 dollars?

The simple answer „none" goes much further simple economical notions of „time delta" and „arbitrage" could ever go.

Cryptocoins cannot be eaten nor drunk. They do not protect from the rain, they do not bring heat – contrary to banknotes which can still be burned on a cold winter day, humans shall be obliged to burn still more and more energy to make the cryptocoin machinery going. Contrary to gold one cannot make jewels or false teeth out of them; cryptocoins arouse no sentiment of beauty. Contrary to credit card payment, one has to wait for at least 10 minutes in case of BTC and 2.5 minutes in case of LiteCoin or TerraCoin to obtain, if lucky, one transaction confirmation (only after 5 or 6 confirmations can be vendor sure that he was not victim of double-spending attack). Contrary to folk believes, the transfer of value in the current cryptosphere therefore definitely does not occur with speed of light.

Thus, as a value-storing asset, cryptocoins have only one principal advantage: there is a limited amount of them. In other terms: they are not for everybody. Not for those living on the continents

where the cryptosphere is absent. Nor for those who jumped too late on this biggest financial bulldozer ever invented. But only for those who think that playing the game with numbers acting of numbers is worth of the limited asset one ever had – time of one‘s life. Only for those who think that having more of anything – even if that anything is, in fact, pure nothing – is an important marker of their social status.

Thus, if posed with question « Cui Bono ? » it may be the case that « economical growth », « market » or « crime » shall be only partial answers, as partial as the answers « gluttony, greed, and vanity» (Dante, 1321). For we believe that it is not completely *hors propos* to state that the structures like Bitcoin serve as opening gates to the world whereby a planetary emergent Artificial Intelligence succeeded to penetrate, for the first time in mandkind’s history, into the realm of our virtues, vices and values.

Barratt, M. J. (2012). Silk road: eBay for drugs. *Addiction*, *107*(3), 683–683.

Bitslog. (2013). The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius. https://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/

Dante, A. (1321). *La Divina Commedia*.

Dingledine, R. (2005). Tor Hidden Services. *Proc. What the Hack*.

Drexler, K. E., & Minsky, M. L. (1990). *Engines of creation*. Fourth Estate.

Garrett, H. (1968). The tragedy of the commons. *Science*, *162*(3859), 1243–1248.

Gilbert, H., & Handschuh, H. (2004). Security analysis of SHA-256 and sisters. *Selected areas in cryptography* (p. 175–193).

King, S., & Nadal, S. (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. http://ppcoin.org/static/ppcoin-paper.pdf

Lopez, J., & Dahab, R. (2000). An overview of elliptic curve cryptography.

Nakamoto. (2008a). Re: Bitcoin P2P e-cash paper. http://www.mail-archive.com/cryptography@metzdowd.com/msg09971.html

Nakamoto, S. (2008b). Bitcoin: A peer-to-peer electronic cash system.

Nietzsche, F. W. (1911). *The Complete Works of Friedrich Nietzsche: Thus spake Zarathustra*.

Percival, C. (2009). Stronger key derivation via sequential memory-hard functions.

Rand, A. (1996). *Atlas Shrugged*. Signet.

Rosenberg, P. (2007). *A Lodging of Wayfaring Men* (2nd éd.). Vera Verba.

Stephenson, N. (2000). *Cryptonomicon*. William Morrow Paperbacks.

Stephenson, N. (2003). *The diamond age*. Spectra.