Pablo R. Velasco González

SUPERABUNDANT DESIGN: FROM WASTE TO CONTROL IN BITCOIN MINING

APRJA Volume 5, Issue 1, 2016
ISSN 2245-7755

Tiziana Terranova draws attention to the necessity of questioning how algorithmically-enabled automation works “in terms of control and monetization” and “what kind of time and energy” is being subsumed by it (Terranova 387). Cryptocurrencies are payment technologies that automate the production of money-like tokens (Bergstra and Weijland) following algorithmic rules to maintain a fixed production rate. Different kinds of energy and residues, which are not always acknowledged, are involved in this process. Here I distinguish between two closely linked layers in the Bitcoin token production: first, an algorithmic layer, which contains the instructions and rules for the creation of bitcoins; second, a hardware layer, which performs and embodies the former. While these layers work together, I will argue that they enact their own kind of logics of energy and waste. I will begin at the more visible end of the production cycle, the hardware layer, where the definition of waste and energy consumption is shared with many electronic devices; then I will trace back its algorithmic layer, which as I argue, follows a different logic.

Hardware layer: Energy, e-waste, and efficiency

A quite introductory video to Bitcoin, the archetypical cryptocurrency, explains that “the bitcoin network is secured by individuals called miners. Miners are rewarded newly generated bitcoins for verifying transactions.” (WeUseCoins). Miners are machines that verify the signed public keys for each transaction and which validate these into blocks in a public registry (i.e., the Blockchain). The job for successfully validating and packing the transactions produces new tokens for the miner, and generates a Proof-of-Work. The former is the result of a ‘puzzle’, which can be then easily checked by any other machine in the network. Since the design of the system seeks a controlled pace, if the coins are generated too fast (because there are more and/or stronger miners) the ‘puzzle’ becomes harder (Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”).[1]

Solving puzzles to produce tokens directly translates into a relevant issue of consumption of energy and production of waste. From the deployment of Bitcoin up until the middle of 2010, mining was a task that any modern CPU could handle, even though the process would push it to its limits and heavily reduce its lifetime. Until mid-2011 the workload moved to GPUs, but was rapidly surpassed by FPGAs (Field Programmable Gate Arrays), which reduced energy consumption while achieving more hashes per second. The next natural step were ASIC miners (Application Specific Integrated Circuit) at the beginning of 2013.[2]

Even though the Bitcoin network was maintained at the beginning by every enthusiast with a computer and some energy to spare, today the mining industry is populated with pools and dedicated farms. This evolution was foreseen in Bitcoin’s design (Nakamoto, “NCML”). In pools, different miners contribute their processing power to calculate a block together. The reward is then distributed among them, usually accordingly to the computational power given, although each pool has its own share protocols. Each one of these clustered miners can have one or multiple ASICs. Mining farms on the other hand are dedicated places that behave in a more or less Fordist fashion, and are even located in old factories or abandoned stores, which house swarms of ASICs (“Bitcoin Mining in an Abandoned Iowa Grocery Store”). The energy consumed in farms is striking. A paper from 2015 estimated that the mining network at the time consumed about the same amount of electricity as Ireland (Malone and O'Dwyer). Although mining units energy efficiency has improved in the last years, the difficulty variable has grown too, and the energy footprint problems of production remain. To cite a specific example, one still operating farm has been told to have 10,000 S3 mining units ("My Life Inside a Remote Chinese Bitcoin Mine"). The Antminer S3 is able to produce 441 Gigahashes per second and consumes 800 Watts per Terahash: that is roughly 4761 Watts in a day, for just one unit. A farm with 10,000 of these units would consume 47,616 Kilowatts a day. Comparing these figures with home energy consuming estimates in the U.S. ("How Much Electricity Does an American Home Use? – FAQ – U.S. Energy Information Administration (EIA)") shows that just this farm consumes 1,571 times more energy than an average household. Mining, today more than ever before, is a race, and reducing the energy footprint is not grounded in pollution awareness, but in cost cutting. As mining units become progressively more energy efficient, they simultaneously become more obsolete. A constant refill of state-of-the-art equipment is necessary to stay in the race. Obsolescence of hardware is not exclusive to the Bitcoin phenomenon, smartphones and all sorts of gadgets are 'recycled' every year as newer versions arrive on the market.[3] According to Michael Bedford Taylor, it took four years to achieve the third generation of mining hardware, and although there are no figures of the number of ASIC units being produced and sold, it would be fair to assume that there is no market comparison with the consumption figures of the smartphones, tablets and other popular devices.

Units by themselves are not more threatening than a colossal mountain of used smartphones, what is menacing is the mono-task logic that produced them. Unlike the smartphone market, mining units do not suffer of a short life because of its hardware resistance, cheap materials or consumption trends, 'planned obsolescence' for ASICs resides in the scarcity model of Bitcoin's design. Tokens have a fixed limit (21 million) and are getting harder to obtain, so the fast production and consumption cycles of the hardware are intrinsic to the system. At least until the mining becomes unprofitable, in such a scenario, the number of miners diminish and with it the difficulty (which, again and recursively, makes the people interested in mining to go up). Difficulty, however, rarely drops, and in the long run describes a stepping curve ("Bitcoin Difficulty Chart – Chart of Mining Difficulty History"), which causes mining hardware to age fast. Being specific circuits optimized for hashing, ASICs do not have a second life. Unlike GPUs, they are useless for any other tasks, which makes them completely worthless after their useful, yet short, life. Since there is no second hand market for mining units, they rapidly contribute to High Tech trashing problems. Electronic waste arguably conforms today about the same amount (in municipal numbers) as plastic packaging waste (Puckett and Smith). Most of the e-waste is recycled in foreign countries because of low labour costs and loose environmental regulations both externally (at least in the U.S. for export of hazardous materials) and internally (waste handling in the host countries). Arguably, around 80% of e-waste is exported to Asia, and 90% of these to China. The hashing power that runs throughout the bitcoin network – i.e. the most and more powerful machine miners – clusters in China too. On a rough estimate ("Bitcoin Hashrate Distribution – Blockchain.info") more than 50% of the hashing power is concentrated in Chinese mining pools and a significant part of the rest is in the U.S., meaning that most of bitcoin's e-waste will eventually end up in Asia.

E-waste is a residual of production that is not reintegrated to capitalist production cycles and thus marks one of the many crises of it, as Jennifer Gabrys argues:

> *Remainder breaks with sustained cycles of productions; it moves us past what might be seen as a Marxian concern with the way raw materials are mobilized for production […] interfering with any notion of a simple feedback loop from production to consumption, remainder calls attention to the after effects and transforms the material arrangements that emerge through the density of our technological and cultural practices. (Gabrys 41)*

Mining waste is an immediate leak of its own cycle. Since it has no secondary use, it is discarded faster than less specialized electronics. It is waste that exceeds production. Mining devices of Bitcoin and other cryptocurrencies insert themselves indiscernibly among the electronic waste in scattered dumps, but its particular monotasking characteristic makes them suitable non-recyclable remainders. Waste in ASIC units follows the general fate of the discarded microchip industry, escaping the loop cycle and disrupting economies and ecologies at the outskirts of capitalism's production. The number of mines and of ASICs in them is obscure. Nonetheless, as said before, the quantity of e-waste coming directly from mining does not compare to the waste produced by other gadgets. The discussion around excess is not so much framed in quantity, however, but in its lifespan and purpose: hardware mining units are limited to the one and only task of solving the Bitcoin puzzle.

To the question of whether Bitcoin mining is a waste of energy the Bitcoin Foundation answers that: "Spending energy to secure and operate a payment system is hardly a waste." ("FAQ – Bitcoin") It is not considered waste as long as the system works. The idea of waste is superseded by efficiency, and annulled in a scenario where the system is fully operative. The substantial empty computational work, energy usage, and e-waste produced in the mining operation has no other goal, and so far no other purpose, than to keep the machine running to produce secure, distributed and artificial scarcity. Within the hardware layer energy is translated into efficiency and residue into excess of production. The former adaptations happen under a discourse concerned with the maintenance of a secure payment system. However, the hardware uses formerly described are mainly underpinned by the rationale of the algorithmic layer. This preceding layer has, as I will argue, its own notions of excess and a different reintegration into the production system.

Algorithmic layer: Designed scarcity, randomness, and control

In this section, I will first argue that this rationale of superabundance is based on a false idea of immateriality. Secondly, the more subtle effect of this mode of production is the reintegration of surplus to production in the form of control.

The efficiency and superior security of the system, eventually translates into compelling symbolic and exchange value. Algorithmic value – the capacity to distribute security in a system via computational power – gains symbolic momentum with growing media attention and generation of controversies. Cryptocurrencies gain recognition, and exchange value grows as their market performance develops, until the tokens of the system can be effectively considered as assets of financial objects. A rush to adopt and exploit the venues follows, as the system becomes prevalent, in great part due to its speculative disposition, which can be exploited as the tokens get exchanged with fiat currencies, creating traditional financial behaviour, like the widely known Bitcoin bubble of 2013. The detonator for the eventual exchange value is, however, the intrinsic value of the algorithms designed to maintain an artificial scarcity.

Modelled scarcity can be considered through what has been defined as "governance by design," which is "the process of online communities increasingly relying on technology in order to organize themselves through novel governance models (designed *by* the community and *for* the community), whose rules are embedded directly into the underlying technology of the platforms they use to operate" (De Filippi). Bitcoin's communities participate in a designed governance, not only in the sense that rules and development are audited and enhanced considering consensus, but in particular because the latter is obtained using the platform (i.e. the branch, fork, and version of the software with a majority of users become the 'de facto' Blockchain). What is more, scarcity is part of the rules enabled by algorithmic governance because while specificities may be open to discussion, the enactment of the rules belongs to a purely algorithmic dimension. For example, regarding scarcity, even though the limit of bitcoins is now fixed to 21 million, this figure is potentially subjected to decisions of the community; however, regardless of the total number of coins, the generation of new ones is algorithmically adjusted to sustain the production in relation to a ratio of difficulty, blocksize and time between each block generation. The resolution framework and enforcement of rules are hardwired to relational data schemes interwoven by discrete steps of precise instructions.[4]

The puzzle analogy is only appropriate within its algorithmic dimension, which means it must be understood not as a toy or a game, but as a problem that must be solved by following a set of rules. More accurately, the puzzle consists of generating hashes (a string of numbers and letters with a defined length) until one of them fulfills the requirements of the variable 'difficulty' level (in the case of Bitcoin, the number of zeroes at the beginning of the resulting hash). This operation, also called a CISO (Constrained Input Small Output) problem is solved by trail and error[5] and due to the random number involved in the process – the 'nonce value' – finding a 'desirable' final hash is a truly exceptional event (Courtois, Grajek, and Naik). Every attempt to come up with a successful hash uses a new random number, thus randomizing the result. Difficulty is hence, in this context, associated with probability and far from tribulation. Regarding Bitcoin, difficulty is an algorithmic adversity.

The difficulty variable (*D*) at 19th September 2015 was set on 59,335,351,233.87, which translates as a 2^25 x *D* number of average hashes to find a block. This means one opportunity to build a block for every 19,909,640,081,173,010,000 (*A*) tried hashes. The only way to deal with the odds involved in this operation is to have a machine capable of generating as many numbers of attempts per second as possible, i.e. an ASIC miner. A state-of-the-art dedicated unit available today can manage to make about 5,500,000,000,000.[6] To calibrate the surplus involved, it is better to think of it in negative terms: unlike the lottery (at which a lonely miner would have better odds) where every non-winner plays a passive role, the miner is a machine that actually uses computational power to actively generate around a sextillion (*A* – 1) useless hashes. I suggest that the algorithmical layer of Bitcoin production is superabundant – underpinned by the idea that digital resources are not bounded – since the mining operation is based in the generation of a sextillion unusable strings.

Designed scarcity is only maintained in a decentralized network via the rules embedded in the above explained excessive use of resources. In a section of her book entitled "Economies of abundance" Gabry's describes Robert Noyce's micro-chip sell strategy.[7] This consisted of selling integrated circuits (which were not as popular at the time) for less than their actual cost. This risky strategy paid out by enhancing the markets and the necessity for microchips as more machines relied on them. In a way, Noyce not only designed a sales strategy, but the pervasiveness of the microchip. Within Bitcoin, the original design of scarcity in a functional distributed system is also the blueprint for the pervasiveness of excessive computational work. Without being a contradiction, in this system scarcity is traded for excess.

Bitcoin and other cryptocurrencies are not systems inherently designed for waste nor significant threats in that sense, and their peculiar mode of production involve a behaviour shared by many algorithmic devices.[8] Yet, they are a pristine example of how the idea of unlimited resources gets embedded into automatized and instrumental apparatuses. Ignoring the more obviously material e-waste, the enormous surplus of the algorithmic layer (a continuous sextillion number operation procedure) is underpinned, to some degree, by the idea that digital informational resources, unlike its more overt material counterpart, *can't* be excessive. There is a rationale of unlimited resources attached to the idea of the digital, in part because is still understood as immaterial. Gabrys reminds us that "waste and waste making include not just the actual garbage of discarded machines but also the remnant utopic discourses that describe the ascent of computing technologies" (Gabrys 4). 'Virtuality' as immateriality, is a live fossil of the rise of computing and its spread onto bewildered crowds. What is more, rather than becoming obviously material due to its more known relations to humans, waste, or servers, digital immateriality hasn't disappeared and, if anything, has become 'post-digital'. That is, an idea of digital superabundance, or unlimited immaterial resources, has become naturalized in our technology, and in our relations to it, to the point that the questioning of the use of *excessive* computing power is redirected to a question of performance. If a system works, the question of excessiveness becomes superfluous.

On the one hand, the design of the system relies on this idea of superabundance, and on the other, the actual algorithmic performance works on its own mode of thought. Bitcoin proof-of-work is a non-human, non-mechanical kind of labour that produces new tokens. Aside from programming and setting up the machines, barely any human labour is involved in the process. Both programming and setting up the machines are not by any means small tasks, and they depend on an assemblage of a huge number of names, discussions, infrastructure, discourses, electricity, investment, and so on. Machines are not built by nature, "they are 'organs of the human brain, created by the human hand'; the power of knowledge, objectified" (Marx 706). However, the production process is executed exclusively by algorithms: labour is predominantly digital, what remains instrumental is only the arrangement of labour. What is more, because the nonce value plays a key role in the process, randomness becomes a fundamental for production. Luciana Parisi argues that this randomness becomes the condition of programming and with it our notion of logic as rationality gets surpassed: "This new function of algorithms thus involves not the reduction of data to binary digits, but the ingression of random quantities into computation: a new level of determination that has come to characterize automated modes of organization and control." (Parisi ix-x) Algorithmic randomness, more than being a systematized reproduction of rules or an applied representation of rationality, works as an outbreak from it, and points to different modes of control.

Algorithms have been successfully integrated to the capitalist economy in notorious ways (Gerlitz and Helmond), mostly as means of production which become valuable as they monetize and accumulate social knowledge, from cognitive means to users behaviour (Terranova 383). Bitcoin is particular in this sense, since it is heavily driven by algorithmic production (native digital labour) of pieces designed to be themselves a novel kind of exchange value. It is tempting to see Bitcoin and other cryptocurrencies as devices attempting to resist the controlled cycles of capitalism production system (an arguably generalized discourse supporting blockchain technologies stands against the abuses of the current economic system). Just as human labour is excessive (as surplus) in a creative way, automation – human knowledge, skills and work absorbed into machines – can develop productive powers not always contained by capitalist economy (Marx 693). Nevertheless, I would argue that the surplus in the algorithmic layer of production (i.e. the excessive operation of mining's algorithmic layer), is not released from the production cycle – as does e-waste – but reintegrated into it, both to the security design of the device and to the scarcity model, as a new means of control for an algorithmically-enabled capitalist economy.

This argument follows Beniger's seminal work to understand the economy of information as means of control. He proposes that the industrial revolution generated a crisis of control, when communication technologies and information processes lagged behind the fast developments of energy technologies and their applications (Beniger). The current economy of information is thus seen as a reaction to the accelerated improvements of manufacturing and transportation of the 19th century, what Beniger calls the "societal control revolution" of the 19th and 20th century. In his view, control is the capability of one agent, human or not, to influence another with a determined purpose. Within communication technologies, this purpose is directed to information processing. Bitcoin's production system is a recoupment of communication over energy. Unlike the residues of the hardware layer escaping the production cycle, the generation of unused hashes of the algorithmic layer are reabsorbed into the system: excessive computation, fuelled by randomness, is *a priori* for performance. The continuous generation of hashes – Bitcoin's instantiation of digital superabundance – is a subtle strategy for both the conservation of a state (scarcity) and for the supervision of a decentralized informational system (a secured ledger). Terranova warns that alongside automation new types of control and strategies to reintegrate surplus are also generated, "[automation] must be balanced with new ways of control (that absorb and exhaust) the time and energy thus released" (Terranova 385). From an algorithm's own logic, the excessive random hashes are not wasted because they are not residue, on the contrary, they remain in the system as enablers of the key states of scarcity and security. In a scenario where Bitcoin's distributed system operates successfully, the algorithmic excess of the system should not be considered waste, but a post-digital element of control.

Notes

[1] I will address relevant details on the functioning of the ‘puzzle’ in the algorithmic layer section.

[2] For a history of Bitcoin mining hardware, up until the end of 2013, see Taylor.

[3] A complex economical and cultural outcome of, among other things, planned obsolescence - an appealing subject for marketing and industrial economics some decades ago, but recently reborn within the scope of ecological awareness (Guiltinan).

[4] Here I am referring to Berlinski’s general definition of algorithm.

[5] Alternatives have been suggested to improve this procedure with less costly computation methods (Courtois, Grajek, and Naik, “Optimizing SHA256 in Bitcoin Mining”).

[6] SP20 Jackson by Spondoolies-Tech (http://www.spondoolies-tech.com/products/sp35-yukon-power-shipping-from-stock).

[7] Noyce was the manager of Fairchild Semiconductor, and then co-founder of Intel, see Berlin.

[8] Much of the cryptography involved in Bitcoin was developed to improve security in different devices, and is used on a day to day basis by generally accepted payment systems (e.g. Europay, Mastercard and Visa) (de Jong, Tkacz, and Velasco González; DuPont).

Works cited

Beniger, James R. *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge, Mass. ; London: Harvard University Press, 1986. Print.

Bergstra, Jan A., and Peter Weijland. “Bitcoin: A Money-like Informational Commodity.” arXiv:1402.4778 [cs] (2014): n.p. arXiv.org. Web. 19 Mar. 2014.

Berlin, Leslie. “The Man Behind the Microchip: Robert Noyce and the Invention of Silicon Valley.” Barnes & Noble. n.p., n.d. Web. 30 Nov. 2015.

Berlinski, David. *The Advent of the Algorithm*. Mariner Books, 2001. Print.

“Bitcoin Difficulty Chart – Chart of Mining Difficulty History.” *CoinDesk*. n.p., n.d. Web. 28 Sept. 2015.

“Bitcoin Hashrate Distribution – Blockchain.info.” n.p., n.d. Web. 28 Sept. 2015.

“Bitcoin Mining in an Abandoned Iowa Grocery Store.” *Motherboard*. n.p., n.d. Web. 28 Sept. 2015.

Courtois, Nicolas T., Marek Grajek, and Rahul Naik. “Optimizing SHA256 in Bitcoin Mining.” *Cryptography and Security Systems*. Ed. Zbigniew Kotulski, Bogdan Księżopolski, and Katarzyna Mazur. Springer Berlin Heidelberg, 2014. 131–144. link.springer.com. Web. 24 July 2015. *Communications in Computer and Information Science* 448.

—. “The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining.” arXiv:1310.7935 [cs] (2013): n. pag. arXiv.org. Web. 23 July 2015.

De Filippi, Primavera. “Commons Governance and Law with Primavera De Filippi” *Common Transitions*. 31 Jul 2015.18 Jan 2016.

de Jong, Eduard, Nathaniel Tkacz, and Pablo Velasco González. “’You Will Live as Friends and Count as Enemies’: On Digital Cash and the Media of Payment.” *Moneylab Reader: An Intervention in Digital Economy*. Ed. Geert Lovink, Nathaniel Tkacz, and Patricia de Vries. Amsterdam: INC Reader 10, 2015, n.p.. Print.

DuPont, Quinn. “The Politics of Cryptography: Bitcoin and the Ordering Machines.” *Journal of Peer Production* 1.4 (2014). Print.

“FAQ – Bitcoin.” n.p., n.d. Web. 28 Sept. 2015.

Gabrys, Jennifer. *Digital Rubbish: A Natural History of Electronics*. Reprint edition. University of Michigan Press, 2013. Print.

Gerlitz, Carolin, and Anne Helmond. “The like Economy: Social Buttons and the Data-Intensive Web.” *New Media & Society* 15.8 (2013): 1348–1365. nms.sagepub.com. Web.

Guiltinan, Joseph. “Creative Destruction and Destructive Creations: Environmental Ethics and Planned Obsolescence.” *Journal of Business Ethics* 89 (2009): 19–28. Print.

“How Much Electricity Does an American Home Use? – FAQ – U.S. Energy Information Administration (EIA).” n.p., n.d. Web. 28 Sept. 2015.

Hughes, John. “Labour, Excess and Utility in Karl Marx.” *The End of Work*. Blackwell, 2007. 63–94. Wiley Online Library. Web. 23 Nov. 2015.

Malone, D., and K.J. O’Dwyer. “Bitcoin Mining and Its Energy Footprint.” Institution of Engineering and Technology, 2014. 280–285. CrossRef. Web. 23 July 2015.

Marx, Karl. *Grundrisse*. Trans. David McLellan. 2nd ed. London (etc.): Macmillan, 1980. Print.

“My Life Inside a Remote Chinese Bitcoin Mine.” CoinDesk. n.p., n.d. Web. 28 Sept. 2015.

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” *Consulted* 1 (2008): 2012. Print.

—. “NCML: Bitcoin P2P E-Cash Paper.” Archive. Cryptography Mailing List. n.p., 1998. Web. 12 Apr. 2014.

Parisi, Luciana. *Contagious Architecture*. MIT Press, 2013. Web. 23 Jan. 2016.

Puckett, Jim, and Ted Smith, eds. *Exporting Harm: The High-Tech Trashing of Asia. Seattle*, Wash.: Diane Pub Co, 2003. Print.

Taylor, Michael Bedford. “Bitcoin and the Age of Bespoke Silicon.” *Proceedings of the 2013 International Conference on Compilers, Architectures and Synthesis for Embedded Systems*. Piscataway, NJ, USA: IEEE Press, 2013. 16:1–16:10. ACM Digital Library. Web. 23 July 2015. CASES ’13.

Terranova, Tiziana. “Red Stack Attack! Algorithms, Capital, and the Automation of the Common.” *Quaderni di San Precario*, February 14 (2014): n. pag. Print.

WeUseCoins. *What Is Bitcoin?* (v2). n.p., 2014. Film.