SUSTAINABILITY OF BITCOINS AND BLOCKCHAIN

Rana Roberto Leonardo[1], Giungato Pasquale[2], Tarabella Angela[3] and Tricase Caterina[4]

[1)]Department of Economics - University of Foggia; [2)] Department of Chemistry - University of Bari; [3)] Department of Economics and Management - University of Pisa; [4)] Department of Economics - University of Foggia

E-mail: roberto.rana@unifg.it; E-mail: pasquale.giungato@uniba.it; E-mail: angela.tarabella@unipi.it; E-mail: caterina.tricase@unifg.it

Abstract

Bitcoin is a digital currency proposed by a developer hided under the pseudonym *Satoshi Nakamoto* in 2009, and it is relied on a peer-to-peer payment system created as an open source software. It is relied on blockchain a distributed and democratically-sustained public register of the transactions. Bitcoin, as well as other digital currencies, has a lower transaction cost and greater security and scalability than fiat money and no need of a central bank. However, in the last years several researchers have relived environmental issues related to the use of this money. On the contrary, the relate technology of blockchain is recognizing as a significant tool contributing to create a more sustainable world. In this context, the purpose of this paper is to describe and evaluate the sustainability of the Bitcoin currency and the blockchain technology considering the environmental and social impacts due to energy consumption, market diffusion compared to fiat currency. Blockchain can reduce and accelerate bureaucracy processes as well as incentivize environmentally friendly behaviour. Under these perspectives, blockchain may show the full applicability of sustainability in the economic, environmental and social sectors.

Keywords

Bitcoin, sustainability, blockchain, energy consumption, cryptocurrency.

JEL Classification

O3

Introduction

Ten years ago, it has been proposed a new digital money created by a hided developer who named with a pseudonym *Satoshi Nakamoto*. This innovative currency bypasses the official way to produce and exchange money and uses a peer-to-peer payment system created as an open source software. At the base of the functioning of bitcoins there is the blockchain technology which generates a distributed and democratically-sustained public register of the transactions. In this way all peer-to-peer money transactions are registered and stored without any changing in a secure way with no need of a central bank. However, recently some scholars have underlined environmental issues related to the releasing of this money (Michel, 2015). On the other hands, they affirm that the relate technology of blockchain

could represent a significant tool contributing to create a more sustainable world. In this context, the aim of this paper is in the first paragraph to illustrate the functioning of this virtual money; while in the second to evaluate the Bitcoin and blockchain technology sustainability, the third part on discussion of the results. It is considered their environmental and social impacts due to energy consumption and market diffusion compared to fiat currency.

Bitcoin and blockchain technology

Bitcoin is the first application of the blockchain technology, which relies on highly secure cryptographic algorithms and sophisticated peer-to-peer technologies. The rate of emission of new Bitcoins or "Bitcoin mining", as it resembles the resource mining such as iron or gold ores, has an inflexible algorithmic limitation starting from 50 unities with an increase rate slowing down constantly: after the issue of 10.5 million Bitcoins, its emission rate will halve, after 15,750,000 Bitcoins, emission rate will halve again and so on, reaching a limited capped value of the total amount of 21 million Bitcoins. Nowadays there are 17,640,713 (April 11, 2019) Bitcoins mined (Karger, 1997). Every block introduces 50 new typologies of coins in the system a number halving about every 210,000 blocks, defining a geometric series which has a capped limit of 21 million of Bitcoins that can be created, following the equation (1).

$$N = \sum_{i=1}^{n} \frac{210{,}000 \times 50}{2^n} \quad (1)$$

In equation (1), N= cumulated number of Bitcoins at time n and the limit for n approaching $+\infty$ is equal to 21 million. Blockchain technology registers all the transactions among Bitcoins owners in its distributed database that holds historical transactional data shared by all nodes through a distributed consensus protocol (Bitcoin, 2019). The blockchain contains the entire history of bitcoin transactions and each node in the network stores a complete or partial copy of the database. New transactions are propagated across the nodes in the network as transfers from a source (input) to a destination (output). Transaction inputs and outputs are not connected to accounts or nor are balanced by a central server or database. Before forwarding a transaction to its neighbors, the node firstly checks the syntax and structure, and verify its validity. In other words, each node verifies the transactions received, propagates only valid transactions, building valid transactions pool. The validity of the transactions collected into a block is verified by computing a cryptographic hash of the block meeting certain constraints (based on the ideas of "Hash-cash"). This verification checksum for the block, is a one-way type as it is easy to compute a hash of a given block, but difficult to compute a block that matches a given hash, and collision resistant as it is difficult to find two blocks that yield the same hash. This work of finding a hash that meets the constraints imposed by the blockchain, is a compute-intensive task executed simply by a brute-force approach. The nodes compete in the network in finding a valid hash as the first node that finds a valid hash, wins the possibility to add the block to the blockchain and propagates the ledger to the network, and it is rewarded with new Bitcoins. The receiving node verify whether the hash is valid, but this task is quite easy and if successful, suddenly it stops the mining process and starts mining for a new block. The node that has verified the block receives a block reward, a certain number of new bitcoins. If multiple nodes simultaneously generate a valid block, a fork temporarily appears in the blockchain, but is resolved as soon as one of the forks contains more blocks and one branch does not receive the consensus of the other nodes. In this manner the computations to find and verify a cryptographic hash of a block during bitcoin mining allows the bitcoin network to gain consensus about the state of transactions (Vranken, 2018).

The question of consensus is crucial for the blockchain operation: the consensus of the blockchain network consists of achieving the unanimous confirmation of the verified transactions by the nodes involved in the blockchain network. An old verified transaction just confirmed will not be tampered with by malicious nodes. The consensus protocol of the blockchain technology consists in the Proof-of-work (POW) in which each node must solve a computationally difficult but easily verified SHA256 problem using its computational power, more simply the task consists in finding a suitable random number called "Nonce" such that the input to the block header metadata and Nonce is computed by SHA256 hash value twice in succession, and the result is less than the difficulty target set in the header of the block. The parameters of SHA256 hash function come from the block header metadata of the current block to be built. Due to the irreversibility of (twice) SHA256 hash, the node must pay enough computational power to perform this Nonce search to the result be as small as possible. The POW consensus induce reliable nodes to create a new block but at the expense of its computational power. A double-spending attack operated by a malicious node should take almost the 51% of the computational power of the entire blockchain network to get successful. For these reasons, bitcoin's mining computational power has surpassed some world's supercomputers, but although the raising of computational power threaten the stability and democracy of the network, the constancy of the mining rate is guaranteed by a mechanism of adjusting values of difficulty in searching with a brute-force approach the right hash for the consensus that operates every 2016 blocks, to ensure an average interval of 10 minutes between linked blocks. This is the mechanisms of the so-called proof of work POW and Bitcoin mining computational efforts caused by the POW mechanism has threatened to the decentralization of Bitcoin network. Researches in the field is directed to solve the issue of increasing computational power by introducing new but reliable consensus. As depicted blockchain technology is based on some core values: decentralization (it rely on a peer-to-peer network and there is no need of a central server), distributed consensus protocol, digital signature and cryptography based on asymmetric public key mechanism, timestamp, peer-to-peer transaction based on decentralized credit in distributed systems (there is no central server or point of control, and all nodes in the network are equal peers), so as to provide a solution to the "double-spending" and "Generals Byzantine" issues (Lamport, 1983; Fan et al. 2013; Fedotova and Veltri, 2006; Reischuk, 1985). Generals Byzantine is the name assigned to a condition of a computer network in which some of the nodes are malicious ones and insert unreliable information but the entire system must agree on a concerted strategy to avoid a system collapse, a situation that recalls that of the Byzantine generals whom treacherously reported false or erroneous news on war strategies to their colleagues. Figure 1 confirms the equation (1) as the cumulated Bitcoin mining, especially in more recent years follow a statistical distribution like the geometric one.

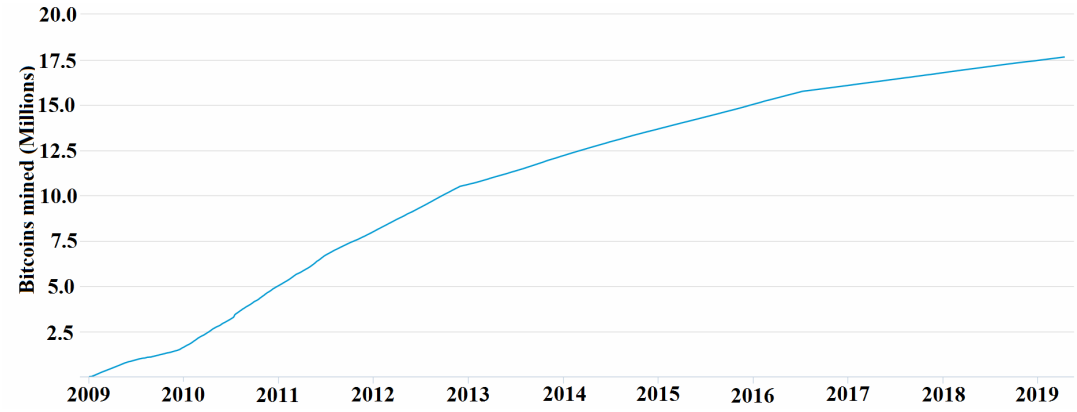

Fig. no. 1 Bitcoins mined (April 11, 2019).

Review of the scientific literature

According to Giungato et al (2017) the Bitcoin system is an environmentally unsustainable since it consumes high amount of energy to mine new cryptocurrency. The International Energy Agency (2017) estimates that the electricity use of Bitcoin data miners may currently be approximately less than $1/40^{th}$ of 1% of global electricity use. This entails a massive fossil fuels consumption and high carbon footprint value contributing to increase global warning above 2°C. In this regards de Vries (2018a) has proposed a Bitcoin Energy Consumption Index which, although is empirical methodology still not validate by scholars, attempts to estimate and to predict power consumed to mine Bitcoin. For instance, he has assessed that the average energy consumption in the 2018 was equal to 38TWh, which correspond to the emissions of 26 million tonnes of CO_2 and to the energy consumed by Israel in the same year (de Vries, 2018b).

Cryptocurrencies are involved also in social aspects as they are particularly attractive for libertarian and anarchist people wanted to see fiat currency removed from the control of a central bank (Golumbia, 2015). Moreover, Bitcoin seems to be unsustainable on economic point of view since the currency transaction system is currently slow allowing about three per day of currency, whereas, for instance, VISA circuit about 6,800. For these reasons the financial world has shown some perplexities of the widespread use of Bitcoins in the future (Mora et al. 2018). Independency is one of the most important characteristics of Bitcoin, but it gives an intrinsic rigidity of process. If a procedure is modified without agreement of user (e.g. from Bitcoin Unlimited-BU to Bitcoin Core-BC), a different cryptocurrency is made. Consequently, according to the logic of market competition this new procedure becomes the only possible and the administration of the previous protocol is abandoned. Moreover, Dodd (2017) affirms that the independency of the Bitcoin system is difficult to achieve since its anarchism is compromised by the way of it operates in practice. In fact, the system fosters the most powerful producers of the currency who increasingly powerful. This encourage an organization to become monopolistic making Bitcoin not a "widespread network" but a way to support strong trend towards the centralization of currency production.

On the other hands Bitcoin could represents an unsustainable virtual money from a social point of view. According to Ver (2014) Bitcoin can be used, for instance, for fraudulent activities by hacking or for illegally trade, drugs, weapons, by criminal associations etc. In fact, it can be used once anonymously an email address to correspond Bitcoin. To improve the legal image of Bitcoins it should be solved this problem. For instance, a positive perspective could arise when considering that Bitcoin will prevents some governments from print money at will for buy weapons. Moreover, their introduction can represent a tool to contrast national policies against bank account holders. For instance, Cypriots recently have begun to buy Bitcoin when the government has proposed to sequester money from their bank accounts.

Results and discussion

The close association among Bitcoin, anonymity and illegal activities is not be true in principle since all transactions are public and permanent on the network. This is not a tool of anonymity but a transparency and traceability system where information pass through the network that does not depend on a centralized agency. In fact, transactions of Bitcoin's required a distributed database that can be considered a public peer-to-peer archive of all the transactions shared among all the participants of the system. The system security is guaranteed by a digital distributed consensus of most of the participants and the information can never be erased since they are stored in a database. This technology called blockchain develop a sort of democratic and digital economy where all the transactions among different

economic entities are traceable. Considering the huge transactions among the business and marketing entities and the bill that companies must pay for maintaining paper-based archives, this technology may open new and challenging opportunities to the economic system. The flexibility of this technology apart from contribute to trigger multiple projects in different economic sectors and improve banking and financial systems it can also has social implications for many organizations and institutions (Tapscott and Tapscott 2017; Nofer et al., 2017). For example, this technology has been proposed to share among doctors and specialists medical record of a patient. This information can be properly conveniently and efficiently tracked and stored in a cloud using immutability and built-in autonomy characteristics of the blockchain. This system based on control of accesses can facilitate exchange of information between research groups and health care institutions as its good controls the access to medical data saved and processed on "cloud structure". Furthermore, it offers secure cryptographic techniques to identify and authenticate users who have access to medical data, keeping a track of all activities carried out (Xia et al., 2017). On the other hands, social sustainability of the technology underlying Bitcoin can be implemented from the innovations generate in the economic system.

Another challenging application of the blockchain technology is in the electricity production and distribution. The diffusion of micro-wind, photovoltaic panels, micro hydro power generation system is rapidly changing the traditional centralized one-directional power grid system towards a micro-grid system at citizen's level. The mass installations and use of these technologies coupled with battery storage and sometimes integrated with devices producing energy from fossil fuels, are transforming citizens from consumers to consumer-producer entities. In this way citizens intent to reduce their electricity bills and to sell their excess power to other local users via smart grids, using innovative technologies such as the blockchain (Green and Newman, 2017). However, the social acceptance of this transition process such as widespread adoption of small-scale technologies (e.g. rooftop installations of solar photovoltaic panels or micro-wind generators) remains unclear. The "citizen's utilities" or consumer-producers as it is called these new entities are growing, needs a technology that ensure information exchange and communications without a centralized server but basing on a distributed public record book of all transactions of energy. For instance, companies such as *Grid Singularity* (https://gridsingularity.com/) or foundation from like *Solar Coin* (https://solarcoin.org/) are using the blockchain technology to manage electricity market among citizen's utilities and microgrids. Therefore, these organizations can help consumer-producers by using a decentralised energy data exchange platform for managing energy and financial transactions base on the blockchain technology (Extance, 2015; Rutkin, 2016).

An interesting application blockchain technology in an advanced state of experimentation consists of DNS (Domain Name System) project management decentralization called "Blockstack" (Ali et al. 2016). DNS is a repository of web address-Internet Protocol address. Blockchain technology represents an alternate mapping DNS-like system that substitute DNS root servers in resolving domain names into IP addresses. The aim of the proposers is substituting DNS servers controlled by both corporations and governments which manage it in a centralized way, to avoid abuse of power in censoring activities, spying and hijacking. Blockchain DNS mapping may improve decentralization, censorship resistance, security, privacy (Ali, 2016). TLS cryptographic protocol assure communications security over nodes of a computer network, and is largely used in web browsing, web-fax, email, voice-over-IP (VoIP) and instant messaging. In the field of ITC security blockchain may improve and decentralize TLS (Transport Layer Security) certificate validation, using the same proof of work of blockchain consensus used in the Bitcoin system. File signatures, voting procedures, stocks and/or bonds shares, notary services, and proof of existence or

other certification released from governmental institutions are interesting applications of the blockchain, as open source experimental applications are developing currently.

Conclusions

In 2009 under the pseudonym of Satoshi Nakamoto a hide developer proposed a digital currency named Bitcoin relied on a peer-to-peer payment system designed as an open source software. Mining and transferring of this virtual money are made under cryptographic connections for this reason Bitcoin is also call as "cryptocurrency". This currency is based on the "blockchain technology" using highly secure cryptographic algorithms and sophisticated peer-to-peer technologies. This technology produces a public ledger of the transactions which is the base for a money distribution sustained democratically. Cryptocurrencies as virtual moneys can be environmental unsustainable since they require enormous amount of energy to sustain and maintain the exchange system of values but the use of these cryptocurrencies could be economically and socially sustainable since it represents a perfectly competitive market, free from inflation and safe from fraudulent activities more and less as fiat currencies. Environmental costs of Bitcoin's mining and maintaining depends on the rate of diffusion into the monetary system, considering only energy costs the system seems to be less consuming than the entire banking system but the overoptimistic replacement of all the actual monetary system into a cryptocurrencies is really an illusion as cryptocurrencies will remain probably a niche entities. Blockchain technology will be an interesting application in sharing framework of medical data, energy generation and distribution among micro-wind, photovoltaic panels, micro-hydro power generating systems related to micro-grids at citizen's level and for management of legal transactions among companies. File signatures, notary services, voting procedures, stocks and/or bonds exchanges, and proof of existence or other certification released from governmental institutions, as contract management among companies are interesting applications of the blockchain, as open source experimental applications are developing currently.

References

Ali, M., Nelson J., Shea, R., Freedman, M.J., (2016). Blockstack: A Global Naming and Storage System Secured by Blockchains, Proceedings of the 2016 USENIX Annual Technical Conference (USENIX ATC '16), Denver, CO, USA, June 22–24, 2016.

Anonimous (2019) Bitcoins in circulation (https://blockchain.info), [last access April 11, 2019].

de Vries, A., (2018a). Bitcoin's Growing Energy Problem, *Joule*, 2, 801–809, [online] Available at: https://www.cell.com/action/showPdf?pii=S2542-4351%2818%2930177-6 [Accessed 4 April 2019].

de Vries, A., (2018b). Bitcoin Energy Consumption Index, [online] Available at: https://digiconomist.net/bitcoin-energy-consumption [Accessed 3 April 2019].

Dodd, N. (2017). The social life of Bitcoin, Theory, Culture & Society. *London School of Economics Research Online*, ISSN 0263-2764, [online] Available at: http://eprints.lse.ac.uk [Accessed 3 April 2019].

Extance, A. (2015) The future of cryptocurrencies Bitcoin and beyond, *Nature.* [online] Available at: http://www.nature.com/news/the-future-of-cryptocurrencies-Bitcoin-and-beyond-1.18447 [Accessed 23 April 2019]. .

Fan J, Yi L T, Shu J W (2013). Research on the technologies of Byzantine system. *Journal of Software*, 24(6), pp.1346-1360.

Fedotova N, Veltri L. (2006). Byzantine Generals problem in the light of P2P computing. Third IEEE International Conference on Mobile & Ubiquitous Systems: Networking & Services 1-5.

Giungato, P., Rana R.L., Tarabella A., Tricase C., 2017. Current Trends in Sustainability of Bitcoins and Related Blockchain Technology. *Sustainability*, 9(12), pp.2214

Golumbia, D (2015), Bitcoin as Politics: Distributed Right-Wing Extremism (April 4, 2015). Geert Lovink, Nathaniel Tkacz, and Patricia de Vries (eds), MoneyLab Reader: An Intervention in Digital Economy, Amsterdam: Institute of Network Cultures. [online] Available at: https://ssrn.com/abstract=2589890 [Accessed 15 April 2019].

Green, J., Newman, P., 2017. Citizen utilities: The emerging power paradigm. *Energy Policy*, 105, pp. 283-293.

International Energy Agency (IEA), (2017). Digitalization &Energy [online] Available at: https://www.iea.org/publications/freepublications/publication/DigitalizationandEnergy3.pdf [Accessed 3 April 2019].

Karger D, Lehman E, Leighton T, Levine M., Lewin M., Panigrahy R. (1997). Consistent Hashing and Random Trees: Distributed Caching Protocols for Relieving Hot Spots on the World Wide Web. Twenty-Ninth ACM Symposium on Theory of Computing. ACM, 654-663.

Lamport L. (1983) The Weak Byzantine Generals Problem. *Journal of the Association for Computing Machinery*, 30(3), 668-676.

Michel, A., Hudon, M. (2015) Community currencies and sustainable development: A systematic review. Ecological Economics, 116, 160-171.

Mora, C., Rollins, R.L., Taladay, K., Kantar M.B., Chock, M.K., Shimada, M., Franklin E.C. (2018). Publisher Correction: Bitcoin emissions alone could push global warming above 2 °C. *Nature Climate Change,* 8, pp. 931–933.

Nofer, M., Gomber, P., Hinz, O., Schiereck, D., (2017). Blockchain. *Business and Information Systems Engineering*, 59(3), pp. 183-187.

Reischuk R. (1985). A new solution for the byzantine Generals problem. *Decision Support Systems*, 1(2), pp.182.

Tapscott, D., Tapscott, A., (2017). How blockchain will change organizations. *MIT Sloan Management Review*, 58(2), pp. 10-13.

Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Curr. Opin. Environ. Sustain.*, 28, 1–9.

Ver R. (2014), How Bitcoin Can Stop War, [online] Available at: http://original.antiwar.com/roger_ver/2014/07/21/how-Bitcoin-can-stop-war/ [Accessed 23 April 2019].

Xia, Q., Sifah, E.B., Smahi, A., Amofa, S., Zhang, X., 2017. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments, *Information (Switzerland)*, 8 (2), pp. 44.

Yu L., Zhao, X., Jin, Y., Cai H., Wei, Bo, Hu, B., (2019). Low powered blockchain consensus protocols based on consistent hash, *Frontiers of Information Technology & Electronic Engineering*, in press, [online] Available at: http://www.jzus.zju.edu.cn/iparticle.php?doi=10.1631/FITEE.1800119 [Accessed 3 April 2019].