future internet

MDPI

Article

Banking on Blockchain: Costs Savings Thanks to the Blockchain Technology

Luisanna Cocco [1], Andrea Pinna [1,*] and Michele Marchesi [2]

[1] Department of Electric and Electronic Engineering, University of Cagliari, 09123 Cagliari, Italy; luisanna.cocco@diee.unica.it

[2] Department of Mathematics and Computer Science, University of Cagliari, 09124 Cagliari, Italy; marchesi@unica.it

* Correspondence: a.pinna@diee.unica.it; Tel.: +39-349-142-0385

Academic Editor: Dino Giuli

Received: 3 May 2017; Accepted: 21 June 2017 ; Published: 27 June 2017

Abstract: This paper looks at the challenges and opportunities of implementing blockchain technology across banking, providing food for thought about the potentialities of this disruptive technology. The blockchain technology can optimize the global financial infrastructure, achieving sustainable development, using more efficient systems than at present. In fact, many banks are currently focusing on blockchain technology to promote economic growth and accelerate the development of green technologies. In order to understand the potential of blockchain technology to support the financial system, we studied the actual performance of the Bitcoin system, also highlighting its major limitations, such as the significant energy consumption due to the high computing power required, and the high cost of hardware. We estimated the electrical power and the hash rate of the Bitcoin network, over time, and, in order to evaluate the efficiency of the Bitcoin system in its actual operation, we defined three quantities: "economic efficiency", "operational efficiency", and "efficient service". The obtained results show that by overcoming the disadvantages of the Bitcoin system, and therefore of blockchain technology, we could be able to handle financial processes in a more efficient way than under the current system.

Keywords: blockchain; banking; efficiency; energy consumption; sustainability; Bitcoin

1. Introduction

Today, sustainable development, green house gas effects and climate change are among the major challenges faced by the mankind, and many organizations, such as financial institutions, are looking to both save money and reduce their carbon footprint.

Information and Communication Technology (ICT) is an essential factor in tackling these challenges. However, if, on the one hand, ICT can help to reduce energy and resource consumption, on the other hand, its ever-increasing usage induces rising demands for energy and resources. The cost of running an IT Infrastructure goes well beyond the cost of acquisition and manpower. It comprises the cost of powering the whole system, and depends heavily on computer software and software process models. There are three main impacts of ICT on the environment (see work by [1]):

> *"First-order impacts are environmental effects that result from production and use of ICT, i.e., resource use and pollution from mining, hardware production, power consumption during usage, and disposal of electronic equipment waste."*

> *"Second-order impacts are effects that result indirectly from using ICT, like energy and resource conservation by process optimization (dematerialization effects), or resource conservation by substitution of material products with their immaterial counterparts (substitution effects)."*

> *"Third-order impacts are long-term indirect effects on the environment that result from ICT usage, like changing life styles that promote faster economic growth and, at worst, outweigh the formerly achieved savings (rebound effects). These effects do not appear sequentially and disconnected. In reality they are nested, which means that second-order effects can only emerge on the basis of first-order effects and third-order effects can only appear as ramifications of second-order effects."*

Effective sustainability initiatives are needed as soon as possible, and environmental sustainability shall play a key role in doing business responsibly and successfully.

Up to now, much effort has been spent to address the environmental aspects of sustainability of computer hardware, but there is much to do in the field of computer software, and software process models. A software product, "Green and Sustainable", should have an economic, societal, and ecological impact, and an impact on human beings as small as possible over its whole life cycle. However, such a software product can be achieved only if all the various stakeholders recognize these impacts, and the whole developing organization is aware of negative and positive impacts that the usage of the software product will likely cause over its whole life cycle.

In past years, many organizations have launched sustainability market initiative to improve environmental performance and environmental management. In addition, many banks are experimenting with the blockchain technology, betting on its ability to promote economic growth by freeing up trade, in order to speed up the rate of technological innovation, and its ability to lead to faster development of green technologies (see work by [2]).

The introduction of blockchain technology may provide substantial energy savings if it may take the place of some of the energy consumptive systems, services and locations that support the fiat currency [3]. Blockchain technology seems to have the potentiality to optimize the global financial infrastructure, dealing with global issues, such as sustainable development, or with asset transfers much more efficiently than current financial systems.

The financial sector incurs in many operative costs in order to efficiently run the whole system. These costs include time and money required to invest heavily in infrastructure, electricity costs to operate and from automated teller machines (ATMs), gas and water consumed by employees and waste produced. In addition, no fiat currency can be created without costs. Periodically in order to guarantee the quality standards for the banknotes in circulation, the worn banknotes are shredded, so, to all operative costs just mentioned, the cost of production of coins and notes and those for the shredding systems have to be added to get an overview of the total cost of the actual financial system.

In contrast, systems based on blockchain technology have only to connect to the network and do not incur electricity costs such as those from ATMs, costs from gas consumed by employees or waste including, for example, paper and toner for printers. Furthermore, in these systems, the production cost of the cryptocurrency is included in the cost of mining activity that comprises also the costs of transaction validation, and, in turn, the distribution costs of new cryptocurrency. This, of course, implies substantial savings with respect to the traditional financial system. The mining activity is the process by which new bitcoins, or, in general, new crypto coins, are generated and new transactions are verified and added to the blockchain, the public ledger which stores the entire transaction history. Anyone who is connected to the Bitcoin network and owns suitable hardware can participate in mining and is called a "miner". In order to secure the network, by adding to the blockchain only the valid transactions, the participants have to solve a computationally difficult puzzle. Specifically, they have to find the so called "Proof of Work" (PoW) burning computational power on useless calculations. Whoever first solves the puzzle gets a reward in Bitcoins, and eventually gets the transaction fees associated with the transactions compiled in the block validated by her.

Two recent articles by [4] and by [5] explore the energy efficiency of Bitcoin. Malmo wrote: *"adopting Bitcoin as a major currency in the next few decades would just exacerbate anthropogenic climate change by needlessly increasing electricity consumption until it is too late"* (Ref. [4]).

Deetman is less pessimistic and categorical than Malmo. He discussed how hashing is related to mining hardware and hence to energy consumption, providing noteworthy "optimistic" and

"pessimistic" energy forecasts. He makes some interesting plots comparing efficiency and product ship dates, and discusses mining trends and scalability. He ended his articles stating that *"Personally, I haven't given up on the idea of distributed network transactions, but a radical rethinking of how these may be secured would be beneficial, be it at least for the environment. Perhaps a system where all miners are rewarded for their pledged surplus in CPU processing power, but the actual hashing is performed only by a few thousand randomly selected and continuously changing CPUs, would be a solution."* (Ref. [5]).

In agreement with this last claim, in this work, we investigate the potentiality of the blockchain technology and the leading role that it could have in addressing the environmental aspects of sustainability. In our opinion, a future evolution and deployment of this technology could revolutionize the banking system.

Blockchain technology, the shared ledger technology based on an open source distributed database, although still in its relative infancy has already triggered much interest, and a lively debate is ongoing about its future progression and the important benefits that could bring in the context of the transfer of assets within business networks.

In traditional business networks, the processes to underpin asset ownership and asset transfer are often inefficient, expensive and vulnerable. The blockchain technology could have, in a not too distant future, a transformative impact on central bank, financial institutions and technology firms.

It could follow in the footsteps of Internet technology, in which the government, industry and academia, beginning with early research on packet switching and the ARPANET (the first network to use the Internet Protocol), contributed to the evolution and deployment of the technology that revolutionized the computer and communication world like nothing before.

Blockchains have the potential to bring great value to several financial service activities, from trade finance to payments, securities settlement, and regulatory compliance. In addition, they could contribute to overcome some traditional banking inefficiencies, such as the foreign exchange (FX) transfer costs and times, to augment existing business networks, and to provide increased discoverability and trust working in cooperation with the banking payment and messaging systems.

A key prerequisite to reach such an interconnected system is achieving a standard way of implementing this technology. In future, we may have multiple ledgers, such as a foreign exchange network and a bond network, which need interoperability to function, just as the internet and intranets share the same technology.

Using blockchain in conjunction with actual banking systems will augment the power operating between counterparties. We potentially may have a common, ubiquitous blockchain, able to reduce the need for intermediaries to validate financial transactions and the friction created in financial networks due to different intermediaries, which often use different technology infrastructures. In theory, such an interconnected infrastructure has the potential to generate significant efficiency gains, reducing duplicative record keeping, eliminating reconciliation, minimising error rates and facilitating faster settlements (see work by [2]).

In addition, such an infrastructure would also be critical to underpinning a future "internet of things". Every device connected to the internet becomes a potential user of banking services, and this infrastructure may enable offering services at much lower cost. Of course, blockchain mining protocols, at least as they look today, are not able to achieve the millisecond response times needed by transactions on the internet of things. A future blockchain with millisecond latency could give devices autonomy, and allow them, for example, to transfer ownership of physical goods without the need to refer to a central management system.

Of course, there are many concerns about scalability, costs, and security to be overcome before blockchain technology moves to widespread usage. There is much concern about whether this technology will be able to achieve the processing speed of an automated clearing house, about the more computational power required to each participating block of a blockchain, and about the actual ability to lower costs compared to traditional payment systems when larger transaction volumes will be involved (see works by [2,6]).

In this paper, we focus on the role of financial and cryptocurrency markets in sustainable development, examining recent trends in banking sector, and possible future events that could shape the role of the blockchain technology in the sustainable development of an integrated financial and cryptocurrency market. We give significant insights about the efficiency of the actual Bitcoin system, showing that the efficiency of the Bitcoin system could increase only by overcoming some of its main limitations, such as the low number of transactions, the block size limit, and the high computational power.

Many works provide food for thought about the potentialities of blockchain technology that if exploited and advanced in an adequate way could bring valid support to the actual financial system, such as the works quoted above [2,6] and a recent report by [7] that estimated that blockchain based systems could bring high potential cost savings. However, to the best of our knowledge, no work focuses on the efficiency of the actual Bitcoin system and on the limitations that hinder a widespread usage of the Blockchain technology, providing an empirical study of the economic and energetic footprint of the Bitcoin system, as we do.

For example, the two works quoted above [4,5] explore the energy efficiency of Bitcoin. The former discuss about the unsustainability of the Bitcoin system claiming that the energy cost of a single Bitcoin transaction could power 1.5 American homes for a day. The latter discusses how hashing is related to mining hardware and hence to energy consumption, discusses mining trends and the scalability. However, both works do not discuss about the limitations that hinder a widespread usage of the blockchain technology in the banking system. In addition, we can cite the work by Vranken [8], who focused on the estimation of the power usage of the Bitcoin network, considering four families of mining hardware. He concluded that the order of magnitude of the energy power is 100 MW. Moreover, we can cite the work by Urquhart [9], who evaluated the economic performance of the Bitcoin system inferring that bitcoin returns are insufficient to cover the energy expenditure of mining operations. Previously, Hayes [10] describe the cost of production of one bitcoin, and O'Dwyer and Malone [11] analysed the bitcoin production cost until 2014 .

All of these works do not provide an analysis of the economic and energetic footprint of the Bitcoin system focusing on the technological limits of the system that hinder the spread of the blockchain technology in the banking sector.

The paper is organized as follows. Section 2 illustrates the sustainability market initiatives in banking and the initiatives, focusing on the use of blockchain technology, which many banks, financial institutes, and industries are carrying out. Section 3 presents the cryptocurrency world, focusing on the many concerns that should be overcome before the blockchain technology moves to a widespread usage in banking system. Section 4 presents an estimation of the mining hardware performances and the power consumption in the real Bitcoin system. In addition, it presents our analysis of the efficiency of the system by computing its economic, service and operational efficiency. Section 5 concludes the paper.

2. Banking on Blockchains: The Fiat World

In banking sector, sustainability market initiatives operate in two key directions [12]:

> *"The pursuit of environmental and social responsibility in a bank's operations through environmental initiatives (such as recycling programs or improvements in energy efficiency) and socially responsible initiatives (such as support for cultural events, improved human resource practices and charitable donations)"*

> *"The integration of sustainability into a bank's core businesses through the integration of environmental and social considerations into product design, mission policy and strategies. Examples include the integration of environmental criteria into lending and investment strategy, and the development of new products that provide environmental businesses with easier access to capital"*

Sustainability strategies try to minimize impact on the environment, starting from making people more efficient, improved recording of environmental key performance indicators, efficient building technology, green travel to sustainable purchasing, and from end-to-end management of resources and waste.

A key concern for banking institutions is climate change and environmental protection to lower the total CO_2 emissions. By working together, banks, their employees, but also service providers and suppliers, can implement sustainability plans more efficiently. The main goals are to get the highest energy efficiency of buildings, employees paper consumption, business travel, but also the running of the cafeterias, where using local products, offering eco-friendly dishes, and working on ways to reduce water consumption should become a common practice. Moreover, in order to minimize environmental footprint, organic waste has to be recycled and converted into a clean source of energy, and renewable energies, to reduce direct and indirect CO_2 emissions, should be more extensively used.

In recent years, there have been many bank endeavours to improve environmental performance and environmental management, launching sustainability market initiatives focused on working together on key matters, such as the development of a joint climate change strategy. In addition, many banks are experimenting with and implementing the blockchain technology, believing in and betting on its ability to lead to faster development of green technologies, in addition its ability to promote economic growth (see work by [2]). The most attention is undoubtedly focused on one of the most interesting aspects of blockchain, "the concept of smart contracts". Smart contracts, encoded in a programming language, are embedded in the blockchain and are executed with the transactions. They may be used, for example, to define the conditions under which the transfer of a bond occurs, giving rise to bond networks.

Thanks to all its potentialities, blockchain technology has triggered much interest and has given rise to several initiatives to advance it, such as the Linux Foundations Hyperledger project [13], the innovation hub blockchain and distributed ledger solutions by Hong Kong's central bank [14], the applications to move money across borders in real-time money using blockchain technology by several banks for examples Santander, UniCredit, Goldman Sachs and Barclays [15], and the initiative by BNP Paribas (Paris, France), the multinational bank, that is working on a blockchain platform in order to enable retail investors to lend money to businesses via an instrument known as a mini-bond [16]. A recent report by [7] estimated that blockchain based systems could bring a potential cost savings of 70% on central finance reporting due to the more streamlined and optimized data quality, transparency and internal controls, of 50% on business operations, such as trade support, clearance and settlement, due to a more efficient and effective clearance and settlement process, of 30–50% on compliance thanks to transparency and auditability of financial transactions, and of 50% on centralized operations due to more robust digital identities and mutualization of client data among participants.

Let us give some insights about the power consumption and carbon footprint, looking at one large financial service german provider, DZ Bank AG (Frankfurt, Germany) and at the whole US banking system.

DZ Bank AG is one of Germany's largest financial service providers. It employs approximately 30,000 people worldwide, of whom 27,800 work in Germany, has more than 1000 cooperative banks and 12,260 branches and over 30 million customers that attest to its importance (see work by [17]).

Since 2013, environmental data for all German offices (see report by [17]) have been collected. In 2015, data highlighted an electricity consumption of 25,520,138 kilowatt hours (kWh), and a heating consumption of 13,152,631 kWh in 2015. In 2015, a reduction in electricity consumption, leading to the drop in CO_2 emission, was registered thanks to the much better management of the electricity generated by hydroelectric plants.

As regards the total CO_2 emissions from electricity and heating, the water consumption, and the volume of waste, including printer and copier paper consumption, envelopes, greeting

cards, sympathy cards, toilet paper, electrical and toner lighting, and so on, −243,444 kilograms (kg), 91,109 cubic meters (m^3), and 534,907 kg were generated, respectively.

Concerning the carbon footprint and costs of the whole US banking system, let us cite an article by [18] entitled "Under the Microscope: The True Costs of Banking". This article describes the results of an analysis about the environmental impact of the world financial access points. The analysis, developed by the CoolClimate Network at the University of California, Berkeley estimated an impact expressed in million tonnes of CO_2/year equal to 383.1 for bank branches, and equal to 3.2 for ATMs, and an energy use expressed in GJ equal to 2.3 billion for bank branches, and equal to 18.9 million for ATMs. This article concludes by making a comparison with the Bitcoin system

> *"At 0.75 million tonnes of CO_2 produced per year, Bitcoin has 99.8% fewer emissions than the banking system".*

3. Blockchain Technology: The Cryptocurrency World

Nowadays, many are the cryptocurrencies and their underlining blockchain technology present in the web, but undoubtedly the most popular are bitcoin and ether. Bitcoin system was created in 2009 by a computer scientist known as Satoshi Nakamoto whose real identity is not known (see work [19]). The Ethereum system was created very recently. It was initially described by Vitalik Buterin in late 2013 and was formally announced by him, in January 2014, at the The North American Bitcoin Conference in Miami, FL, USA [20].

Cryptocurrencies are based on distributed databases for their transactions, and hence on public or shared ledgers, which store the entire transaction history. These ledgers are called the blockchain, because transactions are bundled into blocks. Each block references a previous block, but the first block is called the genesis block.

Blockchain technology is designed as a decentralized peer-to-peer network and does not rely on a single central authority. It uses a broadcast network to propagate transactions and blocks. It broadcasts messages across a network using nodes. Each node has its own copy of the blockchain, which is synchronized with other nodes. No node knows a priori which version of the ledger is valid, and to secure the blockchain against attacks, the cryptocurrency network relies on precise algorithms, consensus mechanisms, such as the PoW in the Bitcoin network and the proof of stake (PoS) in the Nxt network. For a brief overview about the two main consensus mechanisms, PoS and PoW, see work by [21]).

Blockchain technology has triggered much interest around its future progression and the important benefits that it could bring in the context of the transfer of assets within business networks. However, there are many concerns around the blockchain technology, such as its possible and future ability to achieve the processing speed needed for an automated clearing house, to lower costs compared to traditional payment system, and to contain the increase of wasted mining resources when larger transaction volumes will be involved (see works by [2,6,22]).

Looking at PoW as a general consensus mechanism of mining activity (see the next section for its detailed definition), we note many flaws that question its sustainability. The peril of 51% attacks, the ASIC (Application Specific Integrated Circuit) dominance and the high energy inefficiency are the most prominent concerns that could undermine the sustainability of Bitcoin system.

In blockchain technology, the transactions are almost instantaneous but their confirmation needs to be performed by miners, and the average time for the confirmation of a block depends on the consensus mechanism. Bitcoin validates one block every ten minutes, Nxt validates one block every few seconds and Ethereum one every minute [23]. This influences the maximum number of transactions per second (tps) achievable. Today, in Bitcoin system, there are on average 7 tps. In contrast, payment systems like Visa, Mastercard, and Paypal, can afford several thousand tps. For example, VISA handles on average around 2000 tps, and PayPal handles on average around 115 tps [24].

However, looking at the time to complete a transfer in a traditional international bank settlement network, such as Swift and SEPA (Single Euro Payments Area), it depends on the currencies involved, the payment method as well as bank holidays and weekends, and is within 1–4 working days. Banks do settlements between each other only once a day, not including weekends and holidays. In contrast, blockchain technology allows settlements between any different banks in 10 min around the clock, and seven days out of a week. To be fair, a Bitcoin user has to wait about one hour before he can consider its transaction confirmed. In fact, a new transaction can be considered confirmed only after at least five or six block are added in the blockchain. This because block generation process can provoke the creation of a short chain composed by orphan blocks. Orphan blocks are blocks added to the blockchain by a few nodes but that the majority of nodes do not take into consideration. For this reason, orphan blocks are quickly discarded from the blockchain also in nodes which at first considered them as new blocks. For this reason, the time required to have the certainty of confirmation is long at about one hour.

To secure blockchains against attacks, every cryptocurrency network relies on precise algorithms, such as the PoW in the Bitcoin network and the PoS in the Nxt network, and on specific mining hardware.

In the Bitcoin network, each node participating in mining is called a "miner" and has to solve a computationally difficult problem in order to confirm the validity of newly mined blocks. The first node that solves the problem is rewarded with bitcoins. The probability of winning the reward and creating a block is proportional to the total computational power owned. Consequently, an attack against the blockchain is possible only if the attacker owns significant computational resources. The security of the network is supported by the cost of physically scarce resources, and this makes the network inefficient from a resource point of view. Specifically, specialized hardware is needed to run computations, and spending money on electricity is needed to power the hardware.

To increase the probability of winning the reward and creating a block, miners have to participate in an arms race (see work by [25] for more details), that makes prohibitively high the cost of a possible attack, but that makes at the same time the Bitcoin protocol ecologically unfriendly. As a result, alternative mechanisms of block mining that are much less resource intensive have been proposed. Even if the debate is lively and still ongoing, many are convinced that the introduction of the PoS as the consensus mechanism, in place of the PoW, would guarantee a long-term sustainability.

In the PoS algorithms, the probability of winning the reward and creating a block is proportional to a node's ownership stake in the network. The security of the network is guaranteed because, on the one hand, nodes with the highest stake have the most interest to keep the network secure, and, on the other hand, to mount a successful attack, one needs to acquire most of the currency, but this is prohibitively expensive.

PoS offers many advantages with respect to PoW as a mining method. Firstly, it is much more environmentally friendly than PoW. In fact, in order to secure the network, it does not require miners to burn computational power on useless calculations. Secondly, there are no centralization concerns. Indeed, in contrast with PoW, where mining has been essentially dominated by specialized hardware, and there is a large risk that a single large miner will take over and de-facto monopolize the market, PoS is CPU friendly in the long term [23,26].

However, there are also some disadvantages in PoS. For example, the so called "nothing at stake" problem. Miners have nothing to lose by voting for multiple blockchain-histories. This is because, unlike PoW, the cost of working on several chains is small, and miners can attempt to double-spend (in case of blockchain reorganization) "for free" [23,26].

Many have attempted to solve these problems. Peercoin uses centrally broadcasted checkpoints and no blockchain reorganization is allowed deeper than the last known checkpoints (see work by [27]). This system uses a combination of PoW and PoS. It was the first proof-of-stake based coin and was released by Sunny King in 2012. In the PeerCoin system, the PoS is based on a notion of coin age. Coin age of an unspent transaction output is its value multiplied by the time period after it was created. A transaction spending a previously unspent output consumes, or destroys, its coin age (Ref. work by [21])).

Nxt system only allows to reorganize the last 720 blocks. Work by [28] presents a detailed description of Nxt, a 100% proof-of-stake cryptocurrency. Nxt system offers some interesting advantages with respect to the Bitcoin system, such as the potential for reliable instant transactions, increased security, and significant energy and cost efficiency improvements (see work by [29]). In addition, it allows for the processing of up to 367,200 transactions per day. Nxt is resistant to so-called nothing at stake attacks, and since the full token supply was distributed in the genesis block, when an account successfully creates a block, the transaction fees are awarded to that account.

Ethereum developers proposed Slasher protocol that allows users to "punish" the cheater, who mines on the top of more than one blockchain branch [23,26].

Note that Ethereum was designed as a system based on a proof-of-work algorithm named Ethash, and Slasher was never adopted [23,26].

Ref. [30] presented a hybrid mining protocol, based on a consensus mechanism called Proof of Activity (PoA), that relies both on PoW and PoS, and, as a result, takes advantage of the best properties of both consensus mechanisms, giving rise to a better system. Recently, Ref. [31] proposed the Chains of Activity (CoA) system, a pure PoS protocol based on the core element of PoA [30], which aims to overcome the problem of rational forks, caused by the network fragility if the nodes are more rational than altruistic.

Ref. [32] proposed SpaceMint, a cryptocurrency based on proofs of space (PoS), designed to lower setup and overhead costs with respect to the wasteful PoW and to have a fairer reward structure for all miners. The name of this proof stems from the fact that miners dedicate disk space rather than computation power.

In addition to the concern of the Bitcoin protocol being ecologically unfriendly, another concern regards the number of tps in the Bitcoin system today. As already mentioned, this system can do on average around 7 tps. In contrast, payment systems like Visa, Mastercard, Paypal can do several thousand tps. A possible solution, in order to overcome the scalability limitations and the speed of Bitcoin, and to experiment with new working models is that of adding one or more chains, called "sidechains", alongside the Bitcoin blockchain. Sidechains are an innovation proposed and developed by the startup Blockstream, that in early 2015 proposed its prototype sidechain, called "Elements". Such chains allow the creation of new blockchains "pegged" to the Bitcoin blockchain, and their protocols allow value transfer between sidechains and the Bitcoin blockchain that is automatically secured by the Bitcoin mining network. This allows a lower time to validate a block and a different consensus mechanism than those of the Bitcoin protocol. In addition, they allow for managing a more advanced programming environment.

From this possible solution, many projects, such as Segregated Witness and Lightning Network, were generated. Segregated Witness is based on the general concept to separate transaction and signature data. In principle, this could introduce incompatibilities that would change the structure of blocks, causing a split in the Bitcoin network between upgraded nodes and non-upgraded nodes, and hence a hard fork. To avoid this problem, Segregated Witness was implemented by using a clever hack and was rolled out as a soft fork. Specifically, this clever hack marks the transactions as "anyone-can-spend" transactions for non-upgraded nodes, whereas upgraded nodes are redirected to an "add-on block" with signature data (for more details, see the articles by [33,34]). On 15 November 2016, Bitcoin Core version 0.13.1 was released. It is the official introduction of Segregated Witness, which, if activated, enables a number of new features on the Bitcoin network, as well as an effective block size limit increase [35].

Concerning the Lightning Network, it is a decentralized system that allows payments to be securely routed across multiple peer-to-peer payment channels, solving some problems of the Bitcoin network. Specifically, it is a system for instant and high-volume micropayments that today are inconsistently confirmed and the fees render such transactions unviable on the Bitcoin network [36].

4. The Bitcoin System

In order to provide food for thought about the potentialities of blockchain technology looking at them as a valid support for the actual financial system, in this section, we investigated the actual performance of the Bitcoin system with particular attention to its main limitations, such as its ecologically unfriendly protocol, and hence the high computational power required to run the system, which implies high mining hardware expenses, and the low number of transactions, and then the block size limit.

4.1. Ecologically Unfriendly and Friendly Protocols: PoW vs. PoS

As already mentioned, in the Bitcoin network, miners have to run their mining hardware continually, proving that they are spending a substantial amount of money in order to secure the network. In exchange, they gain newly minted bitcoins. Contrary to Bitcoin, in a PoS system, such as Nxt, every one who owns stakes can be chosen to protect the network. The bigger the stake they own, the more often they are chosen to protect the network. With this mechanism, only one or possibly a few computers at a given time run on full power, processing transactions and using energy for validating the transactions, and not for the sake of proving they exist, and spend a lot of money to secure the network.

Ref. [29] presented an interesting comparison between energy and cost efficiency of the Nxt and Bitcoin network. He computed the electricity and the hardware expenses of the Bitcoin network in May 2014. Instead, for the Nxt network, he computed these expenses considering a hypotethical Nxt size equal to that of the Bitcoin network in May 2014.

He analysed the energy and cost efficiency of the Nxt network under the hypothesis that 2500 Cubietrucks will power the network when it gets to Bitcoin's size. A Cubietruck is a forging machine that offers a 1.2 to 1.6 GHz dual core processor. Its value of power consumption, when idle, is equal to 3 W, whereas, at full power, is equal to 18 W. Correctly, he assumed that these forgers use up to 18 W while forging, and consequently that a number of network users equal to 2497 uses only 3 W while idling. As a result, in [29], the total power at a specific time in order to secure the network is equal to 7545 W, and hence equal to 181 kWh per day about 66 MWh per year. Assuming an average rate of 12 cents per kilowatt hour, Czarnek computed a cost of electricity to power the network per day equal to $7937 per year. He also computed the cost of hardware per year, and assuming a cost equal to $100 and a 5-year lifetime for Cubietrucks, he found a cost of hardware per year equal to $50,000.

Regarding the Bitcoin system, he computed the total power consumption on 24 May 2014, starting from the value of the hash rate at that date, equal to approximately 99,300,000 GH/s, and hypothesizing that all miners used on that date the best machines available on the market. Specifically, he picked the Cointerra TerraMiner II, which runs at 1000 GH/s and costs $3500. Assuming hence that 99,300 Bitcoin miners powered the network, he found a power consumption per year equal to about 520,000 MWh, a cost of electricity to power the network per year equal to $62,400,000, and a cost of hardware per year equal to $69,510,000 considering, as in the previous computations, an average rate of 12 cents per kilowatt hour and a 5-year lifetime for mining hardware.

Although the author considered the most energy and cost efficient machines in the market, he highlighted a difference of four orders of magnitude between the Bitcoin and Nxt system, highlighting hence a much higher efficiency of the system using PoS than that using PoW.

Results similar to those by Czarnek for the Bitcoin system emerge also from other works, such as that by [25], who simulate an artificial Bitcoin market, and that by [37], who wrote:

> *"In April 2013 it was estimated that Bitcoin miners already used about 982 Megawatt hours every day. At that time the hash rate was about 60 Tera Hash/s."* See article by [38]).

Adopting the same approach used by [25], based on the fitting curve of the hash rate per US$[H/(s*$)], $R(t)$ and on that of the power consumption [W/H/s] $P(t)$ (defined in the next section), in this work, we compute the electricity and hardware expenditures supported by the Bitcoin mining

network over time, from 30 September 2010 to 31 December 2016. We estimated these expenditures dividing the real total hash rate in the network by $R(t)$. The real total hash rate data was recovered from the blockchain Web site.

Figure 1 shows these expenditures over time in a logarithmic scale. It highlights hardware expenditures increasing over time until 4 October 2014. Then, this increasing trend ends and the hardware expenditures range between $100 million and $382 million, this last value being the highest value reached exactly on 30 October 2014.

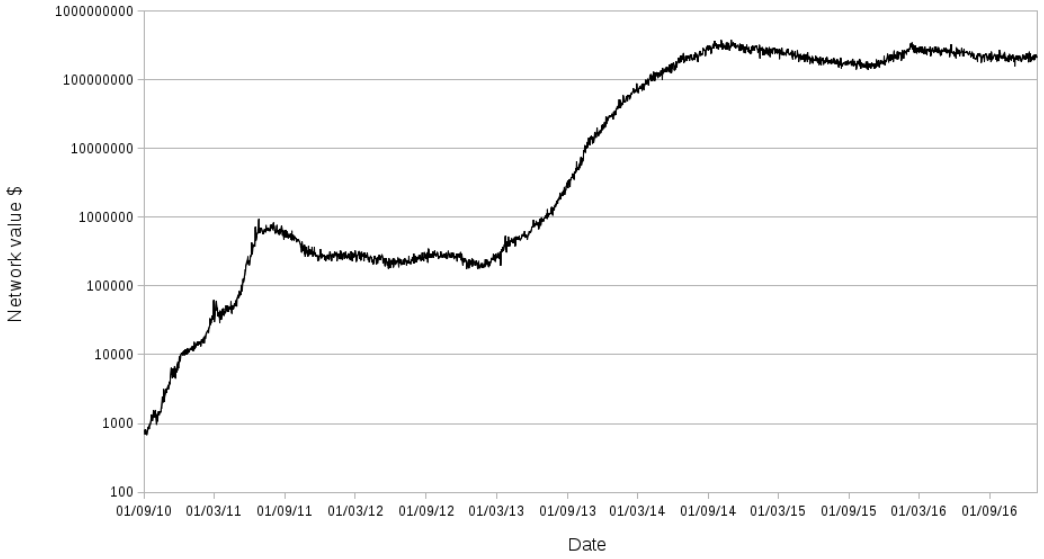

Figure 1. Total estimated investment to create the Bitcoin network .

The electricity expenditures incurred by the network to fuel the Bitcoin system, and hence the power consumption attributable to the Bitcoin system, shows a very similar trend. This is because these expenditures are also computed dividing the real total hash rate in the network by the power consumption $P(t)$.

Using the fitting curve of the power consumption $P(t)$, we estimated the power consumption of Bitcoin system from 1 September 2010 to 31 December 2016. Figure 2 shows this power consumption in a logarithmic scale, and Figure 3 expands the x-axis to highlight the power consumption from 1 October 2015 to 31 December 2016.

Figure 2b shows a power consumption increasing over time until 4 October 2014. On this date, the estimated power consumption was equal to 355.46 MW. Starting from September 2014, this increasing trend ends, and the power consumption ranges between 100 MW and 200 MW (see Figure 3).

Figure 4 shows the annual energy consumption expressed in kWh, from 2011 to 2016. It shows the decreasing trend of the energy consumption in the last three years. This is in agreement with the introduction on the market of mining hardware more and more efficient.

All figures just described highlight that the Bitcoin system, as every system using PoW, an ecologically unfriendly consensus mechanism, incurs high electricity and hardware expenses in order to increase the probability of mining bitcoins by buying hardware more and more powerful.

Despite of this, as already mentioned in the Section 1, all systems based on blockchain technology, both those using PoW and those using PoS, only have to connect to the network and do not incur such electricity costs from ATMs, in costs from gas consumed by employees or in waste including for example paper and toner for printers. Furthermore, in these systems, the production cost of the cryptocurrency is included in the cost of mining activity that comprises also the costs of transaction validation and in turn the distribution costs of the cryptocurrency.

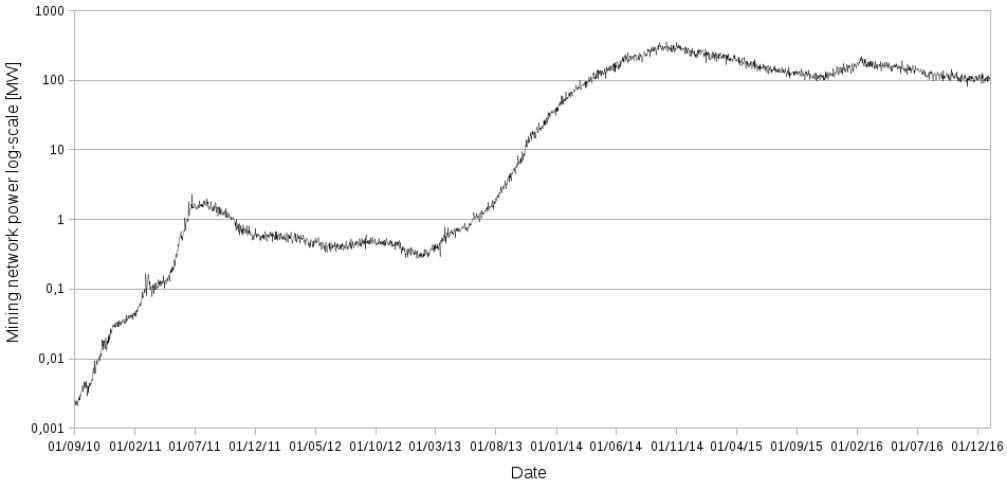

Figure 2. Estimated power consumption of Bitcoin system .

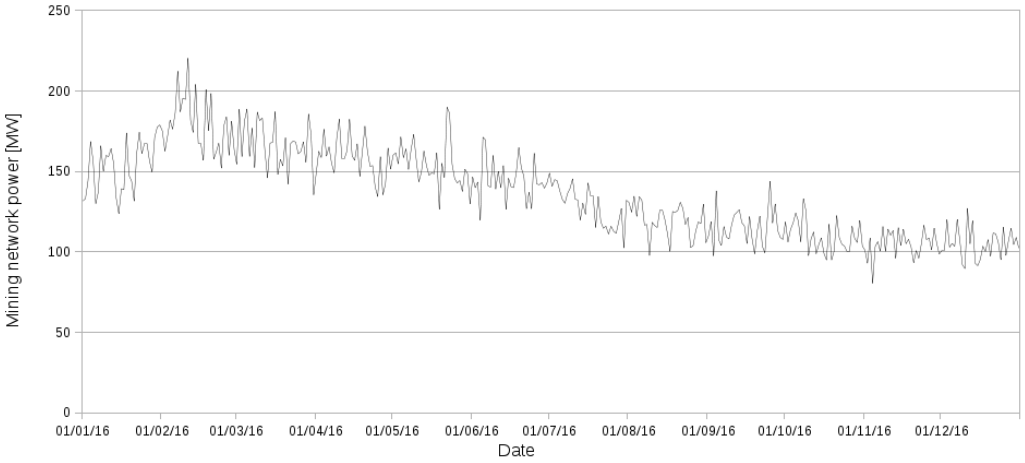

Figure 3. Estimated power consumption of Bitcoin system, from 1 October 2015 to 31 December 2016.

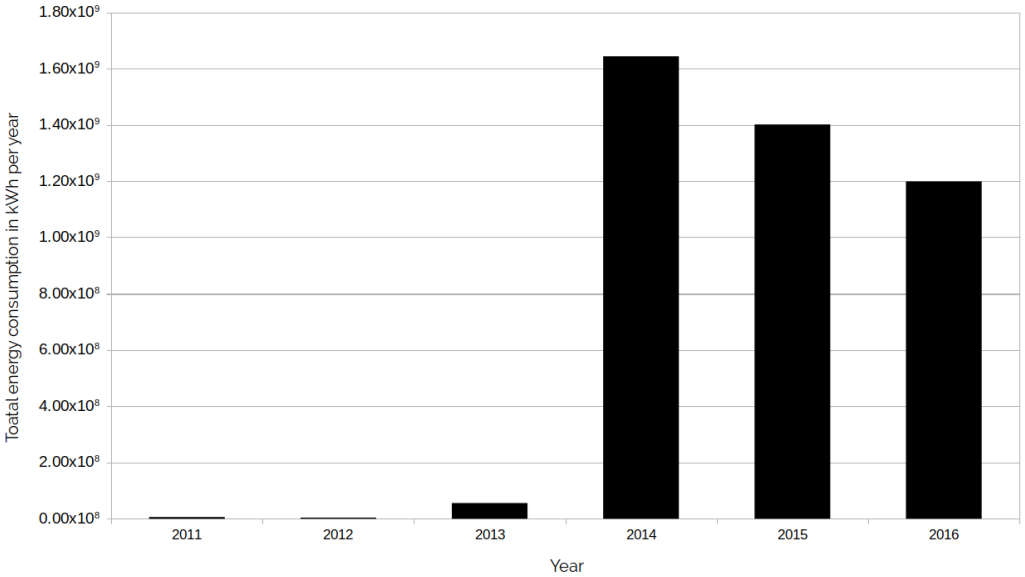

Figure 4. Total energy consumption per year.

Regarding the carbon footprint of Bitcoin system, let us cite an article entitled "Does Bitcoin Have an Energy Problem?" by [39], that gives an estimation of the million tons of CO_2 created by the Bitcoin system when all Bitcoin will be mined.

> *"The total circulation of bitcoin is capped at 21 million, at which point there will be no more mining. Currently, there are just over 14.7 million in circulation. That leaves 6.3 million to be mined. At a cost of $150 a coin and 1.5 tons of CO_2, it will cost nearly a billion dollars and create over 9 million tons of CO_2 just to produce the remaining bitcoins. If we assume that all bitcoins were mined as cheaply as $150 a coin, then it cost $3.1 billion to pay the electricity costs to put all those coins in circulation. It would also have created 31.5 million tons of CO_2".*

This article refers to an article by [40].

The actual Bitcoin system, in agreement with this article, has an impact expressed in million tonnes CO_2/year equal on average to 1, considering a period of 31 years, from 2009 to 2040, 2009 being the year in which the Bitcoin system appeared and 2040 the year in which the system will reach the Bitcoin's cap set at 21 million coins.

4.2. Efficiency

In order to evaluate the efficiency of the actual Bitcoin system, we defined three quantities, "economic efficiency" (EE), "operational efficiency" (OE), and "service efficiency" (SE), starting from the general definition of OE in a business context, defined as the ratio between the input to run a business operation and the output gained from the business.

All of these efficiency measures are heavily affected by the features of the Bitcoin protocol, and specifically from the consensus mechanism unfriendly ecologically, and by the block size limit. Consequently, only future advances in the Bitcoin system, and in general in blockchain technology, will be able to yield a higher efficiency, allowing us to create efficient blockchain based systems.

In order to be able compute these measures, we started by gathering information about the mining hardware that entered the market over time, as in work by [25].

As already mentioned, the people who confirm transactions of bitcoins and store them in the blockchain are called "miners". The first miner who finds a proper hash (he finds the "proof-of-work"), gets a reward in bitcoins, and the successful hash is stored with the block of the validated transactions in the blockchain. Producing a single hash is computationally very easy. Consequently, in order to regulate the generation of bitcoins, the Bitcoin protocol makes the computational complexity of the process needed to find the proof-of-work more and more difficult over time.

As a result, we have witnessed the succession of four generations of hardware, i.e., CPU's, GPU's (Graphics Processing Unit), FPGA's (Field Programmable Gate Array) and ASIC's generation, each of them characterized by a specific hash rate (measured in H/s) and power consumption. Over time, the different mining hardware available was characterized by an increasing hash rate, a decreasing power consumption per hash, and increasing costs.

Starting from the gathered information about mining hardware, we computed the average of Hash Rate and of Power Consumption over time (see Table 1).

We fitted a "best hash rate per $" and a "best power consumption function" and called the fitting curves $R(t)$ and $P(t)$, respectively.

We used a general exponential model to fit the curve of the hash rate, $R(t)$. It is defined as:

$$R(t) = a * e^{(b*t)}, \tag{1}$$

where $a = 6.712 \times 10^6$ and $b = 0.003204$.

We used a similar curve also to fit the curve of the power consumption $P(t)$. It is defined as:

$$P(t) = a * e^{(b*t)}, \tag{2}$$

where $a = 4.636 \times 10^{-7}$ and $b = -0.004005$.

Note that the values of the coefficients a and b stem from the computation of the best exponential fitting curve of the hash rate for Equation (1) and of the average power consumption for Equation (2).

Table 1. Average of Hash Rate and of Power Consumption over time.

Date	Simulation Step	Average of Hash Rate $\frac{GH}{s*\$}$	Average of Power Consumption $\frac{W}{GH/s}$
1 September 2010	1	0.0017	454.87
29 September 2011	394	0.0014	19.8
2 December 2011	458	0.00175	34.4
28 December 2011	484	0.0017	72.575
1 May 2012	608	0.0029	72.575
17 December 2012	835	0.03565	1
10 April 2013	953	0.0194	6
31 May 2013	1004	0.0201	6
15 October 2013	1141	0.1351	3.84
10 December 2013	1197	0.0595	3.84
22 January 2014	1240	0.245	2
4 July 2014	1403	0.583	1.1
23 October 2014	1513	1.6	0.69
30 August 2015	1824	2.756	0.51
1 December 2015	1918	2.666	0.249
1 May 2016	2070	4.746	0.273
30 September 2016	2221	8.465	0.099

4.2.1. Economic Efficiency

We defined the "economic efficiency" (EE), as the ratio between the value of bitcoins expressed in US$ mined by the power consumption of 1 kWh.

In order to compute this quantity, data about the number of bitcoins generated over time and the bitcoin price were recovered from the "blockchain.info" web site. Data about the power consumption are computed by using the fitting curve defined in Equation (2), and data about the real hash rate are recovered from the "blockchain.info" web site.

Figure 5 shows the trend of economic efficiency over time. We can observe that EE reached the highest values in the period between April and August 2013. In particular, the economic efficiency reached its highest value, exactly equal to US$63.47 per kWh, on 9 April 2013.

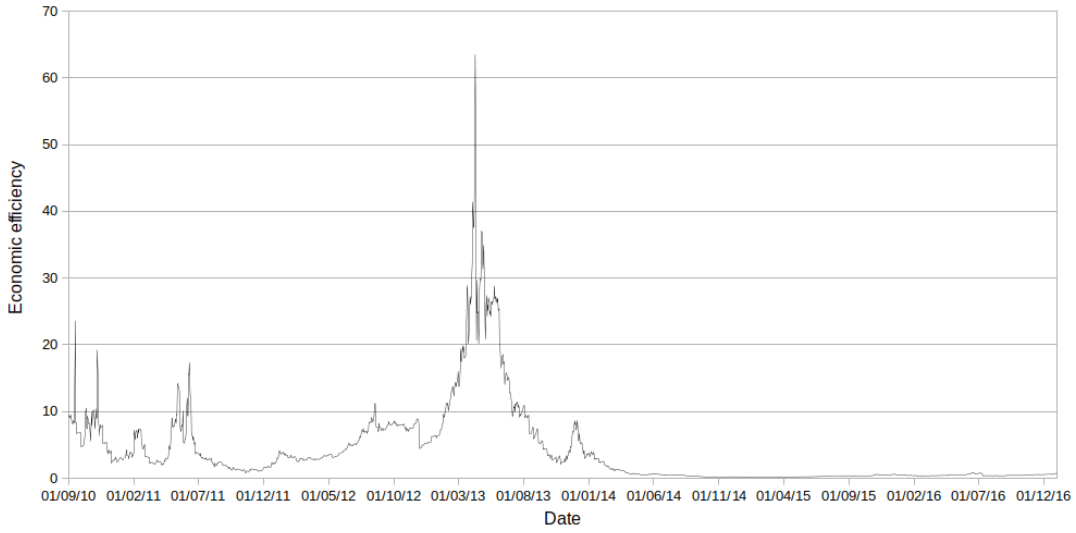

Figure 5. Economic efficiency expressed in US$ per kWh from 1 September 2010 to 31 December 2016.

The trend of EE is strictly linked to the rapidly growing interest in the Bitcoin system that steadily drove the prices higher and higher. Bitcoin price, starting from negligible values, reached values of about $140 in April 2013 and about $1000 in November 2013. This price increase caused the growing trend of EE until 10 April 2013 and also its fall from 10 April onwards. In fact, such a huge interest brought an arms race for acquiring efficient and specialized mining hardware. From 10 April 2013 onwards, EE started to decrease due to the dramatic increase of the total hash rate and power consumption also, in conjunction with the halving of the bitcoin mining prize, which halved two times in this period. Specifically, Bitcoin's block reward was halved the first time, from 50 to 25 bitcoins in November of 2012, and the second time, from 25 to 12.5 bitcoins on 9 July 2016. Figure 6 shows the trend of the EE, expanding the x-axis to highlight its values from 1 October 2015 to 30 September 2016. During this period, the EE ranges between 0.3 and US$0.85 per kWh. In this figure, it is also possible to observe the effect of the last halving on the trend of EE, which falls sharply on that day.

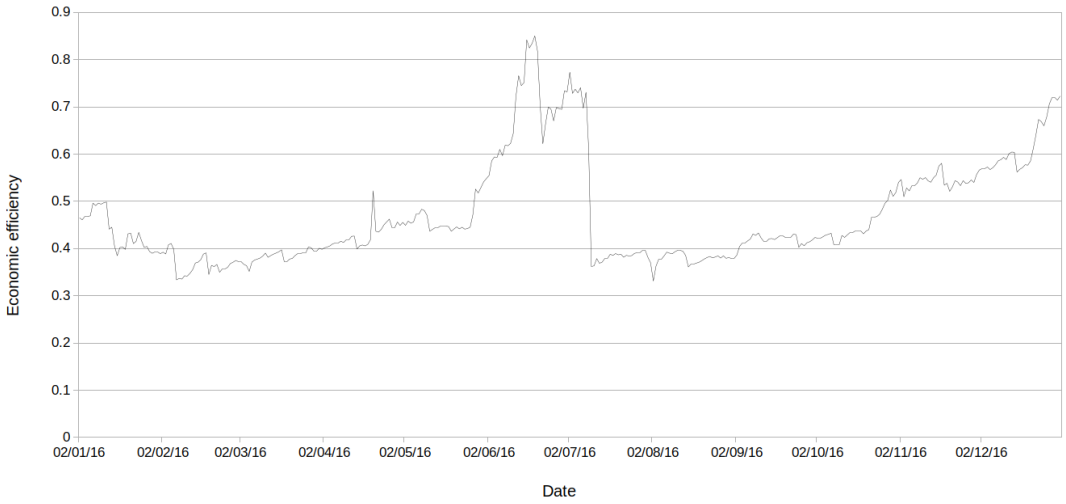

Figure 6. Economic efficiency expressed in US$ per kWh from 1 October 2015 to 31 December 2016.

Note that the EE is also strictly linked to the energy cost, and indeed the majority of hashing power of Bitcoin network is concentrated among a handful of Chinese mining pools [41], given that China is one of the countries where there are the lowest energy costs. Thus, if we take into account the variable component of the energy cost for Chinese industrial consumers, which ranges between 0.0525 and 0.0825 US$/kWh (0.35 a 0.55 Y/kWh). Nnote that, in China, the variable component of the energy cost has to be added to the fixed component, which depends on the stipulated contract. and compute the profit per kWh, we obtain a value that ranges between $0.2475 and $0.7675. Compared to China, in Italy (which is the European country with the highest electricity price), the average energy cost for non-domestic users is equal to 0.2119 US$/kWh [42], and, as a result, the profit per kWh is much lower, exactly between $0.0881 and $0.6381.

4.2.2. Operational Efficiency

We defined the "operational efficiency" (OE), as the ratio between the value of voluntary fees and the energy cost of a transaction. In general terms, it is defined as the ratio between the output gained by a business and the input to run a business operation. We defined this efficiency as the ratio between the value of the voluntary transaction fees and the energy cost of a transaction. The transaction fees are the fees paid to the miner who validates the block that includes that transaction. They are voluntary and are an incentive for miners in order to include a transaction into the next block. However, a miner can accept a transaction and include it in the new block also without any reward in return. Thus, a person posting a bitcoin transaction can include any fee, or none at all, in the transaction.

We computed this efficiency using the monthly average of total daily transaction fees, the daily energy consumption obtained through Equation (2) and the real data about the hash rate. Figure 7 shows the trend of OE.

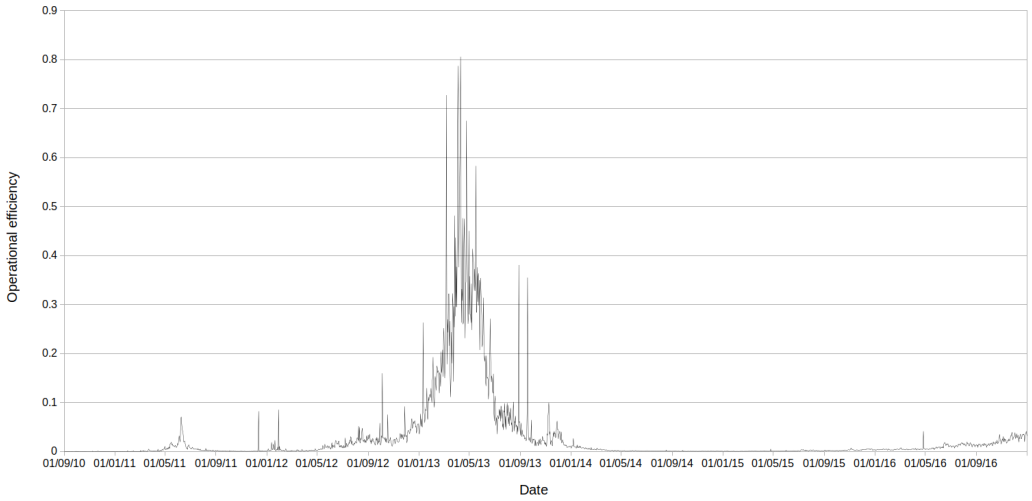

Figure 7. Operational efficiency from 1 September 2010 to 31 December 2016.

Its value increased until 10 April 2013, when OE reached its highest value, 80.6 US$ cents per kWh, but then it started to decrease.

Figure 8 shows the trend of the OE, expanding the x-axis to highlight the OE from 1 October 2015 to 31 December 2016. Note that, after the period in which OE decreases, from about July 2015 onwards, the OE started to slowly increase.

This increasing trend seems to follow the importance that the fees have over time. When the number of bitcoin generated will approach the value of 21 million, there will be no fixed mining reward anymore, and the only mining reward will be that associated with the transaction fees. As a result, only a growing OE trend will guarantee the survival of the Bitcoin system.

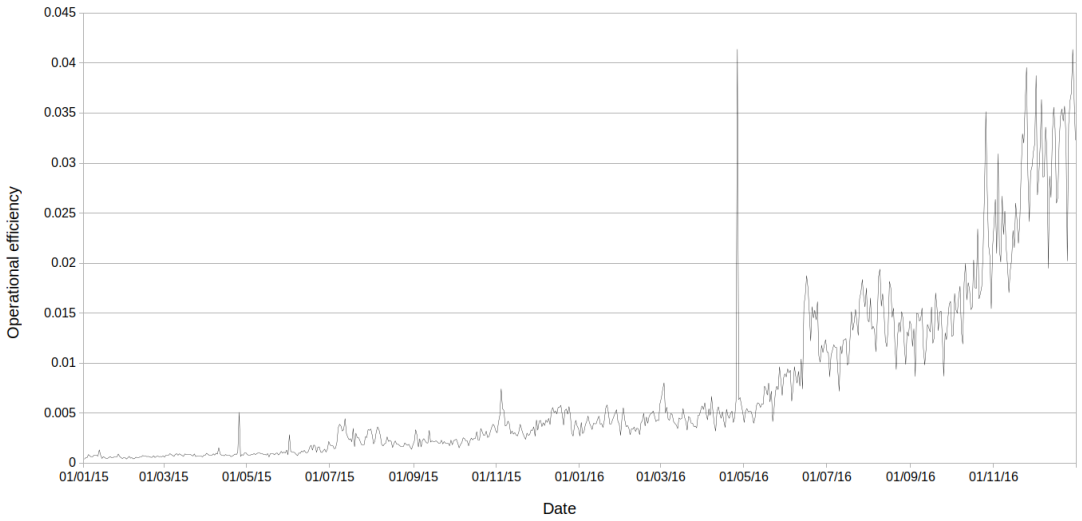

Figure 8. Operational efficiency from 1 October 2015 to 31 December 2016.

4.2.3. Service Efficiency

We defined the "service efficiency" (SE), as the ratio between the number of transactions validated by the power consumption of 1kWh. In order to compute the SE, data about the number of transactions validated over time were recovered from the "blockchain.info" Web site, and data about the power consumption were computed as described for EE in Section 4.2.1.

Figure 9 shows the SE over time and Figure 10 shows its value limiting the max y-axis to 10 transaction per kWh. Until September 2013, the SE ranged between one and 10 transactions per kWh. Then, SE drastically decreased, keeping its values always under one transaction per kWh. The worst estimated SE dates back to 4 October 2014, when it had a value equal to 0.0098 transaction per kWh. From 1 October 2015 to 31 December 2016 (see Figure 11), SE ranges from 0.04 to 0.14 transaction per kWh.

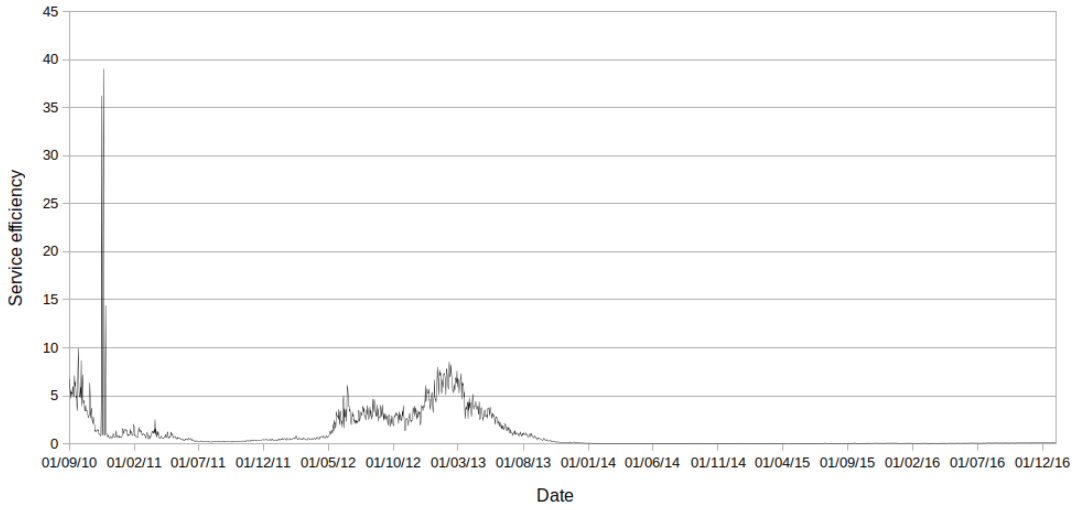

Figure 9. Service efficiency expressed in number of transactions per 1 kWh from 1 September 2010 to 31 December 2016.

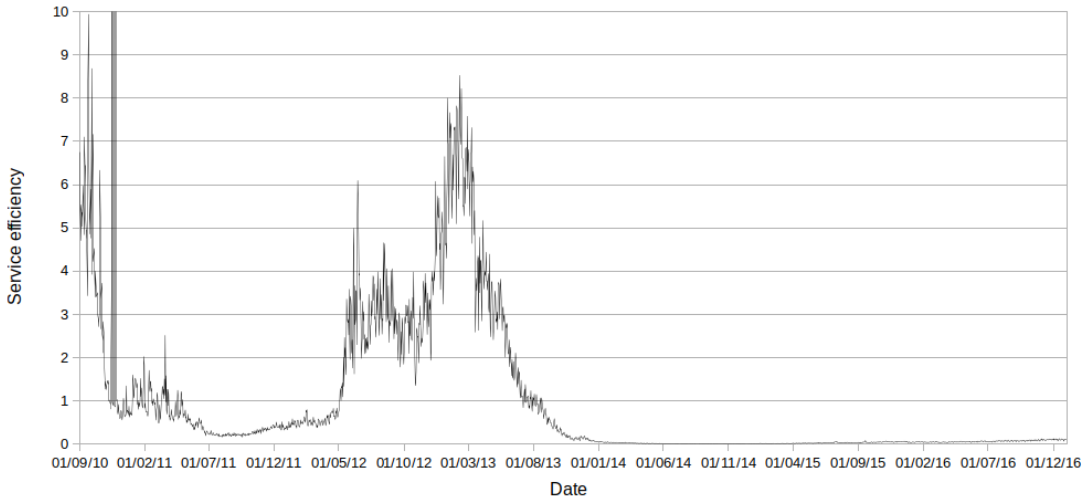

Figure 10. y-axis zoom of the service efficiency expressed in number of transactions per 1 kWh from 1 September 2010 to 31 December 2016

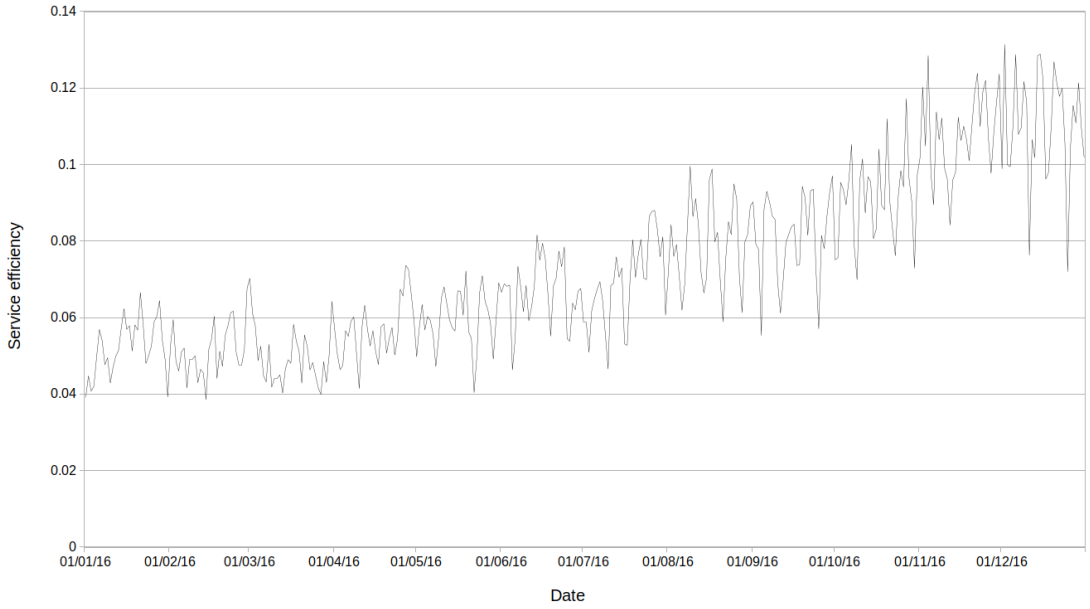

Figure 11. Service efficiency from 1 October 2015 to 31 December 2016.

Note that the block size limit and the time interval between blocks are two limitations that compromise the service efficiency of the Bitcoin system. When we reach the block size limit, the number of transaction per block cannot increase anymore. As a result, the energy consumption per transaction will increase whenever a new miner machine will be added to the network, and hence it will increase when the hashing capability of the network increases.

Figure 12 shows the number of transactions per block, which is steadily increasing. The increasing trend ended started from about September 2015, when the number of transactions approached the imposed block size limit, equal to 1 MB.

In agreement with the considerations made in the first sections of this paper, the performed analysis confirms that the efficiency of the Bitcoin system, and hence the proposed efficiency measures could increase only by overcoming some of the Bitcoin system's main limitations, such as the low number of transactions, and then the block size limit, and the high computational power. They do not aim to demonstrate that the actual Bitcoin system is more efficient than the actual financial system but only to provide food for thought about the potentialities of blockchain technology that, if exploited and advanced in an adequate way, could bring a valid support to the actual financial system. Consequently, the research activity should move in this direction, increasing the number of transactions per block and decreasing the computational power required to run the system. Only overcoming these limitations can the introduction of the Bitcoin system, and, precisely, the introduction of the blockchain technology into the actual financial infrastructures, allow us to deal with global issues much more efficiently than current financial systems.

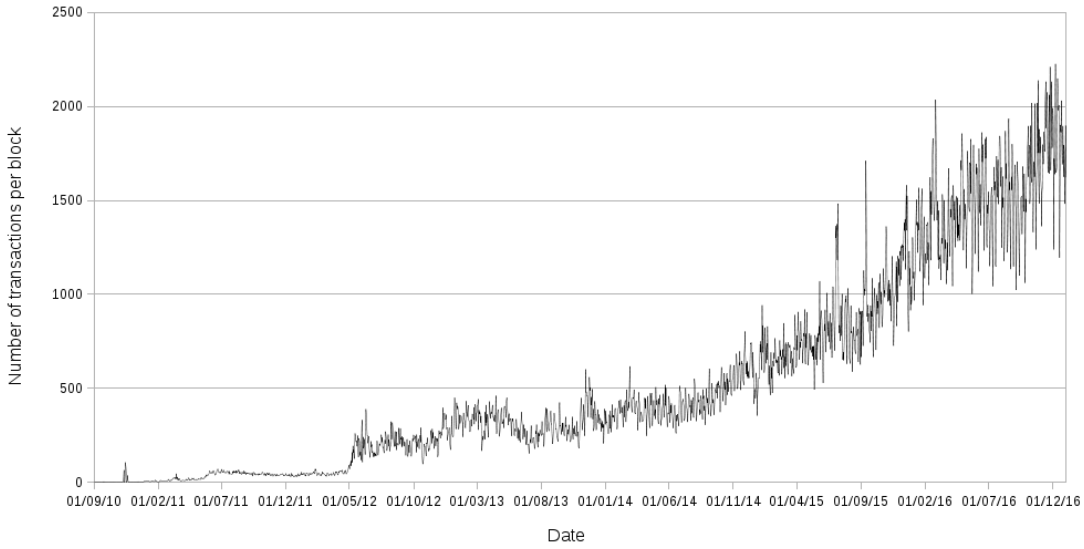

Figure 12. Daily number of transactions per block.

5. Conclusions

Blockchain technology has the potentiality to optimize the global financial infrastructure, enhancing the efficiency of current financial systems. This paper looks at the challenges and opportunities of implementing blockchain technology across banking and capital markets. In order to analyse the Bitcoin system during the years, we took into account its evolution. We considered that mining hardware has evolved over time, passing trough CPU, GPU, FPGA, and ASIC. In particular, we considered two of its features: the hash rate and the power consumption. Using two fitting curves, we computed the "best hash rate per \$", $R(t)$ and the "best power consumption function", $P(t)$. We defined three quantities: "economic efficiency" (EE), "operational efficiency" (OE), and "efficient service" (SE).

First, we found that the EE, defined as as the ratio between the value of bitcoins mined by the power consumption of 1 kWh, is characterised by a strong variability because it is influenced by the Bitcoin popularity and the power consumption of the network. It is currently growing, thanks to the growing of the Bitcoin price.

Second, we found that the OE, defined as the ratio between the value of voluntary fees and the energy cost of a transaction, is currently growing, indicating that fees are becoming more and more important to assure the sustainability of the Bitcoin system. In fact, mining operations will be remunerated only until the sum of circulating bitcoins reaches 21 million.

Finally, we discussed the SE, defined as the ratio between the number of transactions validated by the power consumption of 1 kWh, which describe how much electricity the network spends to perform its main service, i.e., to wire bitcoin. Because transaction blocks are limited in size (1 MB), the number of transactions per block is limited, and the SE can not increase.

In a nutshell, all of our results show that the overall efficiency of the Bitcoin system can increase only after overcoming its main limitations: the low number of transactions per block and the too high computational power that it currently needs. In conclusion, our work provides a reflection on the potential of blockchain technology that could bring good support to the financial system. By sorting out the highlighted problems, the introduction of the Bitcoin system and, more in general, the introduction of blockchain technology to financial infrastructures could allow for addressing financial issues much more efficiently than current financial systems.

Author Contributions: Luisanna Cocco, Andrea Pinna and Michele Marchesi conceived paper and analysis on Bitcoin system. Andrea Pinna performed data analysis. Luisanna Cocco wrote the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Naumann, S.; Dick, M.; Kern, E.; Johann, T. The GREENSOFT Model: A reference model for green and sustainable software and its engineering. *Sustain. Comput. Inf. Syst.* **2011**, *1*, 294–304.
2. McLean, J. *Banking on Blockchain: Charting the Progress of Distributed Ledger Technology in Financial Services*; Technical Report; Finextra Research Ltd.: London, UK, 2016.
3. Bradley, J. The Energy Efficiency of Bitcoinm. 2016. Available online: https://www.cryptocoinsnews.com/energy-efficiency-bitcoin/ (accessed on 9 January 2017).
4. Malmo, C. Bitcoin is Unsustainable. 2015. Available online: http://motherboard.vice.com/read/bitcoin-is-unsustainable (accessed on 12 January 2017).
5. Deetman, S. Bitcoin Could Consume as Much Electricity as Denmark by 2020. 2016. Available online: http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020 (accessed on 12 February 2017).
6. Lees, A.; King, M. *World Payments*; Technical Report; Capgemini and The Royal Bank of Scotland: Dublin, Ireland, 2017.
7. Accenture. *Banking on Blockchain, A Value Analysis for Investment Banks*; Technical Report; Accenture Consulting: Dublin, Ireland, 2017.
8. Vranken, H. Sustainability of bitcoin and blockchains. *Curr. Opin. Environ. Sustain.* **2017**, *28*, 1–9.
9. Urquhart, A. The inefficiency of Bitcoin. *Econ. Lett.* **2016**, *148*, 80–82.
10. Hayes, A. A Cost of Production Model for Bitcoin. 2015. Available online: https://ssrn.com/abstract=2580904 (accessed on 23 January 2017).
11. O'Dwyer, K.J.; Malone, D. Bitcoin mining and its energy footprint. In Proceedings of the 25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), Limerick, Ireland, 26–27 June 2014; pp. 280–285.
12. International Institute for Sustainable Development. Sustainable Banking. 2016. Available online: http://www.iisd.org/business/banking/sus_banking.aspx (accessed on 9 January 2017).
13. Linux Foundation. Linux Foundation's Hyperledger Project Announces 30 Founding Members and Code Proposals to Advance Blockchain Technology. 2016. Available online: https://www.linuxfoundation.org/news-media/announcements/2016/02/linux-foundation-s-hyperledger-project-announces-30-founding (accessed on 12 January 2017).
14. Rizzo, P. Hong Kong's Central Bank to Test Blockchain. 2016. Available online: http://www.coindesk.com/hong-kongs-central-bank-test-blockchain/ (accessed on 3 February 2017).
15. Yu, H. What Wall Street's Obsession With Blockchain Means for the Future of Banking. 2016. Available online: http://fortune.com/2016/07/10/wall-street-blockchain-technology-banking/ (accessed on 3 February 2017).
16. Rizzo, P. French Bank BNP is Testing Blockchain for Mini-Bonds. 2016. Available online: http://www.coindesk.com/french-bank-bnp-testing-blockchain-mini-bonds/ (accessed on 12 January 2017).
17. Roth, M. *Sustainability Report*; Technical Report; DZ Bank: Frankfurt , Germany, 2015.
18. McCook, H. Under the Microscope: The True Costs of Banking. 2014. Available online: http://www.coindesk.com/microscope-true-costs-banking/ (accessed on 24 January 2017).
19. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Technical Report. 2009. Available online: www.bitcoin.org (accessed on 24 June 2017).
20. Ethereum Community. History of Ethereum. 2016. Available online: http://ethdocs.org/en/latest/introduction/history-of-ethereum.html (accessed on 17 January 2017).
21. BitFury, G. Proof of Stake Versus Proof of Work. Technical Report. BitFury Group. 2015. Available online: http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf (accessed on 10 February 2017).
22. Ametrano, F.M. Hayek Money: The Cryptocurrency Price Stability Solution. Available online: https://ssrn.com/abstract=2425270 (accessed on 13 August 2016).
23. Buterin, V. On Stake, 2014. Available online: https://blog.ethereum.org/2014/07/05/stake/ (accessed on 16 January 2017).
24. Bitcoinwiki. Scalability. Available online: https://en.bitcoin.it/wiki/Scalability (accessed on 15 January 2017).

25. Cocco, L.; Marchesi, M. Modeling and Simulation of the Economics of Mining in the Bitcoin Market. *PLoS ONE* **2016**, *11*, e0164603.
26. Buterin, V. Slasher: A Punitive Proof-of-Stake Algorithm, 2014. Available online: https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/ (accessed on 16 January 2017).
27. King, S.; Nadal, S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Technical Report. 2012. Available online: https://peercoin.net/assets/paper/peercoin-paper.pdf (accessed on 5 April 2017).
28. Nxt. Whitepaper: Nxt. Technical Report. NXT Wiki. 2016. Available online: https://nxtwiki.org/wiki/Whitepaper:Nxt (accessed on 24 June 2017).
29. Czarnek, M. Nxt Network Energy and Cost Efficiency Analysis. 2014. Available online: https://www.scribd.com/document/254930279/Nxt-Network-Energy-and-Cost-Efficiency-Analysis (accessed on 20 January 2017).
30. Bentov, I.; Lee, C.; Mizrahi, A.; Rosenfeld, M. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake; In *Cryptology ePrint Archive*; Report 2014/452; Succinct Computational Integrity and Privacy Research: Tel Aviv, Israel, 2014.
31. Bentov, I.; Gabizon, A.; Mizrahi, A. Cryptocurrencies Without Proof of Work. In *Financial Cryptography and Data Security: FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers*; Clark, J., Meiklejohn, S., Ryan, Y.P., Wallach, D., Brenner, M., Rohloff, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; pp. 142–157.
32. Park, S.; Pietrzak, K.; Kwon, A.; Alwen, J.; Fuchsbauer, G.; Gazi, P. Spacemint: A Cryptocurrency Based on Proofs of Space. In *IACR Cryptology ePrint Archive*; International Association for Cryptologic Research (IACR): New York, NY, USA, 2015; Volume 2015, p. 528.
33. Wirdum, A.V. The Segregated Witness Timeline: From Idea to Adoption in Six Steps. 2016. Available online: https://bitcoinmagazine.com/articles/the-segregated-witness-timeline-from-idea-to-adoption-in-six-steps-1461255570 (accessed on 23 January 2017).
34. Redman, J. The Segregated Witness Concept: A 'Turning Point' for Bitcoin? 2016. Available online: https://news.bitcoin.com/segregated-witness-concept-turning-point-bitcoin/ (accessed on 23 January 2017).
35. Wirdum, A.V. Segregated Witness Officially Introduced with Release of Bitcoin Core 0.13.1 2016. Available online: https://bitcoinmagazine.com/articles/segregated-witness-officially-introduced-with-release-of-bitcoin-core-1477611260 (accessed on 23 January 2017).
36. Poon J.; Dryja T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments 2016. Available online: https://lightning.network/lightning-network-paper.pdf (accessed on 24 January 2017).
37. Courtois, N.; Grajek, M.; Naik, R. The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining. 2014. Available online: http://arxiv.org/pdf/1310.7935v3.pdf (accessed on 25 January 2017).
38. Mark, G. Virtual Bitcoin Mining Is a Real-World Environmental Disaster. 2013. Available online: www.Bloomberg.com (accessed on 18 January 2017).
39. Carterand, J. Does Bitcoin Have an Energy Problem? 2015. Available online: http://blog.acton.org/archives/82688-does-bitcoin-have-an-energy-problem.html (accessed on 9 January 2017).
40. Quiggin, J. Bitcoins Are a Waste of Energy-Literally. 2016. Available online: http://www.abc.net.au/news/2015-10-06/quiggin-bitcoins-are-a-waste-of-energy/6827940 (accessed on 30 January 2017).
41. Gautham. The Dominance of Bitcoin Network by Mining Pools 2016. Available online: http://www.newsbtc.com/2016/06/30/dominance-bitcoin-network-mining-pools/ (accessed on 30 January 2017).
42. Autorita per l'energia elettrica, il gas ed il sistema idrico. Prezzi medi finali ai clienti non domestici nel 2015 per livello di tensione (Italian) 2016. Available online: http://www.autorita.energia.it/it/dati/eep254.htm (accessed on 12 January 2017). (In Italian)