future internet

MDPI

Article

An Agent Based Model to Analyze the Bitcoin Mining Activity and a Comparison with the Gold Mining Industry

Luisanna Cocco [1,*], Roberto Tonelli [2] and Michele Marchesi [2]

[1] Department of Electric and Electronic Engineering, University of Cagliari, 09123 Cagliari, Italy
[2] Department of Mathematics and Computer Science, University of Cagliari, 09124 Cagliari, Italy; roberto.tonelli@dsf.unica.it (R.T.); michele@diee.unica.it (M.M.)
* Correspondence: luisanna.cocco@diee.unica.it

Received: 14 November 2018; Accepted: 27 December 2018; Published: 2 January 2019

Abstract: In this paper, we present an analysis of the mining process of two popular assets, Bitcoin and gold. The analysis highlights that Bitcoin, more specifically its underlying technology, is a "safe haven" that allows facing the modern environmental challenges better than gold. Our analysis emphasizes that crypto-currencies systems have a social and economic impact much smaller than that of the traditional financial systems. We present an analysis of the several stages needed to produce an ounce of gold and an artificial agent-based market model simulating the Bitcoin mining process and allowing the quantification of Bitcoin mining costs. In this market model, miners validate the Bitcoin transactions using the proof of work as the consensus mechanism, get a reward in Bitcoins, sell a fraction of them to cover their expenses, and stay competitive in the market by buying and divesting hardware units and adjusting their expenses by turning off/on their machines according to the signals provided by a technical analysis indicator, the so-called relative strength index.

Keywords: cryptocurrencies systems; Bitcoin; gold; sustainable development; blockchain technology; agent-based modeling

1. Introduction

A cryptocurrency is a digital asset, a medium of exchange, that uses cryptography to secure the transactions and to control the creation of new coins. Bitcoin is the most popular cryptocurrency, but today, there are hundreds of cryptocurrencies, often called Altcoins.

In general, a cryptocurrency is based on public and shared ledgers, called blockchains, which are distributed databases that bundle the transactions into blocks. Cryptocurrency systems are decentralized peer-to-peer networks that do not rely on a single central authority. To secure the network against attacks, these networks rely on precise algorithms known as consensus mechanisms. A consensus mechanism is the mechanism that secures the network and validates the transactions, generating at the same time the coins. In the cryptocurrency's network, trust comes from the consensus algorithms, which have to be created in such a way that they are very, very hard to cheat.

In the Bitcoin network, the consensus mechanism adopted, called "Proof of Work" (PoW), questions the sustainability of the network due to the peril of 51% attacks, the ASIC (Application Specific Integrated Circuit)dominance, and the high energy inefficiency. Many are convinced that the introduction of a different consensus mechanism, such as Proof of Stake (PoS), in place of the PoW, would guarantee long-term sustainability. Others are convinced that a system using PoS as the consensus mechanism creates the problem of a monopoly (refer to the article by Young [1]). In a PoW network, all actors belonging to the community—miners, developers, and other members—have

voting power when important changes to the system have to be implemented. Instead, in a PoS network, major stakeholders have this voting power. This centralization of voting power undermines the main feature of the blockchain technology, that is the absence of a central authority.

In order to avoid this problem, many alternative consensus mechanisms have been proposed. These alternative mechanisms use the PoS as the basic algorithm and offer additional security, assigning the voting power according to precise "target values" depending not only on the balance of the account, but also on other variables, such as the number of blocks an account has gone without making a transaction, or the number of transactions someone has made and/or received over a certain number of blocks (see the article by Cointelegraph.com [2]).

Bitcoin has much in common with gold, an asset that has been the store of value for years, resisting technological, political, and economical changes, and overcoming the test of time, it has become a very popular asset class over the years. Instead, Bitcoin is new, only eight years old, but it is exhibiting gold-like properties (see [3]). In terms of rarity and scarcity, transportability and, above all, infrastructure, Bitcoin may be considered superior to gold. Bitcoin is rarer and scarcer than gold. Bitcoins are rarer because the whole Bitcoin system is set up to yield just 21 million Bitcoins, and when the 21 million cap of Bitcoins is reached, no Bitcoins will be generate any longer. Opposite to Bitcoin, the availability of gold depends on the supply-and-demand cycles, and a high demand for gold gives incentives for the gold miners to find and mine more.

With respect to transportability—which refers to how easy it is to move from one location to another the goods to complete an exchange—that of Bitcoin is higher than that of gold bullion because it is transportable like a digital file.

With respect to the infrastructure—which refers to the whole system that generates and distributes an asset—in the actual Bitcoin system, in order to produce Bitcoins, one has only to connect to the Bitcoin system. Anyone who is connected to the system and owns suitable hardware can participate in mining by solving a computationally-difficult mathematical problem. The one who first solves the puzzle gets a reward in Bitcoins. People who confirm transactions of Bitcoins and store them in the blockchain are called "miners", and their activity is called mining. The mining cost of Bitcoin is included in the cost of the mining activity that comprises the costs of transaction validation and, in turn, the distribution costs of the cryptocurrency.

Instead, in the gold mining industry, in order to produce an ounce of gold, one has to move through several stages. It is necessary to discover where the gold deposits may be, analyzing rock samples to determine if the gold actually exists, the size of the deposit, and the quality of gold. If the identified deposits makes mining worthwhile, infrastructures must be constructed before the actual mining takes place. Finally, when the gold reserves in the mine are exhausted, the mine is not abandoned, but a reclamation project starts to return the land to its previous natural state. All these stages, taking the metal ore from the Earth and converting it into gold bullion, are quite expensive. In addition, they are becoming more and more expensive given that gold is becoming both harder to mine and more scarce.

Looking at sustainable development, Bitcoin mining infrastructure allows one to better address the environmental aspects of sustainability, and given the high interest in this technology, in the near future, there may be an ecologically-friendly Bitcoin protocol that allows one to reduce the mining cost in order to have a system that allows one to save money and to reduce the carbon footprint (see [4]). In addition, the blockchain technology has the ability to promote economic growth because it allows free trade, which speeds up technological innovation, leading also to the development of green technologies (see the work by McLean [5]). The introduction of this technology may provide substantial energy savings if it takes the place of some of the energy-consumptive systems, services, and locations that support the fiat currency (see [6]).

Opposite to Bitcoin, the carbon footprint of gold will continue to increase, given that most of the energy used in mining comes from non-renewable fossil fuels, like diesel, which hardly is replaceable with renewable resources (see [7]). In addition, the gold industry has caused environmental and health

problems for decades to miners and mining communities. For example, there is an increasing concern for the health of miners and mining communities related to the mercury exposure, a toxic metal used in small-scale gold mining, and for the ecosystems' degradation due to mining land use [8,9].

Therefore, looking at the total mining costs, such as production costs, economic costs, environmental costs, and social costs, of these two assets or "safe havens", probably a wide spread of Bitcoin could allow us to better address the environmental aspects of sustainability and to have substantially higher savings than gold [8–12].

In this paper, we present an analysis of both mining processes and propose an agent-based artificial market model to simulate the Bitcoin mining activity. The model proposed is a modified version of the model proposed in a work by Cocco et al. [13].

The agents present in the Bitcoin market are the miners that validate the Bitcoin transactions, get a reward in Bitcoins, and sell a fraction of their by mined Bitcoins to cover their expenses. They stay competitive in the market buying new mining hardware units and divesting the old ones. In addition, they adjust their expenses by turning off/on their machines according to the signals provided by a technical analysis indicator, the relative strength index, which forecasts price movements by analyzing past price data. Note that in this model, the Bitcoin price is an exogenous variable and is equal to the real Bitcoin price.

The model is able to simulate the total hash rate in the real Bitcoin market—hence the estimated number of tera-hashes per second that the Bitcoin network is performing—and compute the total expenses sustained by miners, showing that adjusting the expenses by turning off/on a fraction of the mining hardware units allows miners to achieve a higher total wealth per capita. Before concluding, the paper gives some insights on the power consumption incurred by the Bitcoin system, hypothesizing the use of PoS as the consensus mechanism.

The paper is organized as follows. Section 2 presents the lifecycle of gold. Section 3 describes the artificial market model to simulate the Bitcoin system using PoW. It illustrates some simulation results, providing the cost per mined Bitcoin both in a system using PoW as the consensus mechanism and in a hypothetical Bitcoin system using the PoS consensus mechanism. Finally, Section 4 concludes.

2. Gold Mining Industry: The Gold Lifecycle

The mining lifecycle of gold comprises several stages: generative stage, exploration stage, evaluation stage, development stage (mine construction), production stage, mine closure and rehabilitation stage, monitoring and evaluation stage, and finally, lease relinquishment stage.

The generative, exploration, and evaluation stages represent the beginning stages of any gold mining project. Discovering where gold deposits may be, analyzing the promising areas, and performing drill testing are the activities performed in these stages. To pin down potential deposits of gold, the companies engage geologists and other competent figures. At these early stages, methods such as geological surface mapping and sampling, geophysical measurements, and geochemical analysis are often applied.

Once mapping, sampling and measurements, and analysis data are collected, the process moves forward to the design and planning stage, to evaluate if and how the project can be safe, environmentally sound, economically viable, and socially responsible.

If a worthwhile mining activity is associated with the identified area, the construction stage takes place, and the infrastructure is built. This stage involves building roads, creating processing facilities and environmental management systems, building employee housing, and other facilities. It can take a long time, up to five years, between the time when the promising area is discovered and the time when the actual mining activity takes place.

Once the infrastructure is built, the production stage starts. The two most common methods of mining are that of surface mining and that of underground mining. The chosen method is determined mainly by the characteristics of the mineral deposit and the limits imposed by safety, technological, environmental, and economic concerns (see [14]). At this stage, gold is recovered; the

ore is extracted from rock using adequate tools and machinery and processed in order to separate commercially-valuable minerals from their ores. This is an on-site processing and is relatively simple for low-grade ore. Once ore is processed on-site, the processing off-site takes place. The ore is transported to smelting facilities to extract the metal from its ore and to produce bars of bullion ready for sale.

Once having completed the production stage, the process moves forward to the final stages. When the mining site has been exhausted, it is necessary to close the site and to dismantle all facilities on the property. In order to return the land to its original state, a rehabilitation program starts to ensure public health and safety, minimize environmental effects, remove waste and hazardous material, preserve water quality, stabilize land to protect against erosion, and establish new landforms and vegetation (see [14]).

As a consequence, extracting metal ore from the Earth and converting it into gold bullion is quite extensive and requires much front-end investment and time.

According to experts, the reporting of the gold industry's cost is unclear, and probably, the real costs to produce an ounce of gold have not been clearly described yet. Let us start looking into the history of gold cost reporting in the industry (see [15,16]).

In the mid-1990s, the industry introduced "cash costs" to shed light on the gold industry's costs and showed that the reputation of the reporting of such costs was an embarrassment and an utter joke. Cash cost essentially took into account the cost to dig gold out of the ground and sell it, but ignored other costs such as sustaining capital and General and Administrative expenses (G&A expenses). Therefore, this cost became increasingly ridiculous as industry cost inflation accelerated over the past decade. In 2012, the senior gold companies working with the World Gold Council created a new measure. They created a new industry standard, All-In Sustaining Costs (AISC). This measure takes into account sustaining capital, which becomes bigger and bigger as mines get older and grades decline, along with the G&A expenses, but it does not include costs such as project capital or dividends.

In an article published by providentmetals.com [17], the author wrote that the gold mining costs were underestimated until the 1990s. In those years, the values of these costs fluctuated between $500 and $800 per ounce and did not consider for example the expenses to buy and repair the equipment and those to run the whole company. After the introduction of the AISC metric, these costs increased. The estimate passed over $1000 per ounce (see [17] and [7]), and these costs are expected to increase over time since gold is becoming more and more scarce and much harder to mine. As the density of the mineral declines, it is necessary to extract more ore to produce the same amount of gold. Consequently, also the carbon footprint of gold is expected to increase since most of the energy used in mining comes from non-renewable fossil fuels (see [7]). In 2005, Barrick and Newmont, two of the world's largest gold producers, burned an average of 17.2 gallons of fuel to produce one gold coin, and in 2015, after only 10 years, they burned an average of 32 gallons of fuel to produce one gold coin [18].

3. Bitcoin Mining Activity: The Model

The model presented in this work is a modified version of the model proposed in the work by Cocco et al. [13]. The proposed model presents an agent-based artificial cryptocurrency market in which agents, specifically miners, mine and sell Bitcoins to cover their expenses.

In this market, miners belong to mining pools; hence, they mine at least a fraction of Bitcoin (The number of Bitcoins b_i mined by the i^{th} pool per day is computed easily by knowing the number of blocks discovered per day, and consequently knowing the number of new Bitcoins B to be mined per day. Refer to [13] for more details.) at each time t; the number of miners is constant over time (The number of miners in the market is assumed constant because the probability that the new agents entering the market are miners is lower and lower over time (see work [13]). This number is computed following the approach proposed in [13], in which the authors assumed that in the early days of the Bitcoin system, these people were the people who traded Bitcoins, considering that the maximum number of people that owned Bitcoins in 2017 was equal to 10 million, that the maximum possible

number of people that could be interested in the future in Bitcoin trading is equal to 2.5 billion (see [19]).); and finally, the Bitcoin price is an exogenous variable.

3.1. Miners

All miners present in the market at the beginning of the simulation, hence at the initial time $t = 0$, hold a precise fiat cash, $c_i(0)$ expressed in U.S. dollars, and a precise crypto cash, $b_i(0)$ expressed in Bitcoins, where i is the trader's index (the wealth distribution, both in crypto and fiat cash, of miners follows a Zipf law (see [13] for more details and [20])).

Miners are in the Bitcoin market aiming to gain by generating Bitcoins thanks to their hashing capability. We modeled the hashing capability of miners starting from the total value of the hash rate present in the network at the beginning of the simulation. Knowing this value, we distributed it among the miners in a way proportional to their wealth [21,22]. After having assigned to each miner his/her hashing capability, we are able to compute their ability to validate blocks and their gains in Bitcoins.

Miners in the market own a precise number of Antminer S9 units; hence, they are initially endowed with a precise value of hashing capability $r_i(0)$, which implies a specific electricity cost $e_i(0)$. Antminer S9 is the mining hardware machine that dominated the Bitcoin ASIC market for most of 2017 and 2018. Since we analyzed the Bitcoin mining costs from 1 January 2017–31 May 2018, the assumptions above are reasonable.

Note that we considered the electricity expenses as being equal to 70 percent of the total Bitcoin mine's expenses [23,24], and as a result, knowing the electricity expenses, we computed the expenses to set up and maintain the mines as 30 percent.

Over time, miners can improve their hashing capability by buying new mining hardware units and by divesting the old mining hardware units. In addition, they can improve their profitability by adjusting their hashing capability—strictly linked to their maintenance and electricity expenses—as a function of the real Bitcoin price trend.

3.1.1. First Strategy: Buying New Hardware Units and Divesting Old Hardware Units

Miners can improve their hashing capability by buying new mining hardware, investing both their fiat and crypto cash. Consequently, the total hashing capability of the i^{th} trader at time t, $r_i(t)$ expressed in (H/s), and the total electricity cost $e_i(t)$, expressed in \$ per day, associated with his/her mining hardware units, are defined as in [13], respectively, as:

$$r_i(t) = \sum_{s=t_i^E}^{t} r_{i,u}(t) \tag{1}$$

and:

$$e_i(t) = \sum_{s=t_i^E}^{t} \epsilon * P * r_{i,u}(s) * 24 \tag{2}$$

where:

$$r_{i,u}(t = t_i^E > 0) = \gamma_{1,i}(t) c_i(t) R \tag{3}$$

$$r_{i,u}(t > t_i^E) = [\gamma_{1,i}(t) c_i(t) + \gamma_i(t) b_i(t) p(t)] R \tag{4}$$

Let us briefly describe the variables in the equations above (for more details, refer to the work by Cocco et al. [13]). R is the hash rate, which can be bought with one US\$, expressed in $\frac{H}{sec*\$}$, and P is the power consumption, expressed in $\frac{\text{W}}{\text{H/s}}$. Since we assumed that in the near future, no technological breakthrough occurs, we assumed that Antminer S9 is the only mining hardware machine in our artificial market. Therefore, the value of hash rate, R, is fixed to $5.833 \times 10^9 \frac{\text{H}}{\text{s}*\$}$, and the power consumption, P, is fixed to $0.099/10^9 \frac{\text{W}}{\text{H/s}}$. The number 24 represents the total hours in a day. $r_{i,u}(t)$ is the hashing capability of the hardware units u bought at time t by the i^{th} miner, and $\gamma_{1,i}$ and γ_i

represent the percentage of the miner's cash allocated to buy it and that of the miner's Bitcoins to be sold for buying the new hardware at time t, respectively. ϵ is the fiat price per Watt and per hour. It is assumed equal to 8.5×10^{-5} \$, considering the cost of 1 kWh is equal to 0.085 \$ (The fiat price per Watt and per hour refers to the electricity cost in Sichuan. This is because, today, Chinese mining pools control more than 70% of the Bitcoin network's collective hash rate [25,26]. China is the undisputed world leader in Bitcoin mining. It manufactures most of the world's mining equipment; massive mining farms are located in China, as its electricity tariff is one of the lowest in the world. The largest concentration of miners is located in Sichuan, a province in southwest China, estimated to be about 30 percent of the total. Electricity in Sichuan costs around \$0.08–\$0.09/kWh for commercial and industrial consumption [27]. Benefiting from a low electricity tariff is extremely important because electricity typically accounts for 60–70 percent of a Bitcoin mine's expenses [23,24]. In addition, the Chinese exchanges used to lead the world in terms of volume; Antpool is a Chinese-based mining pool, maintained by Bitmain, an ASIC manufacturer).

Every miner buys new hardware units if its fiat cash is positive and divests the hardware units older than one year. The decision to buy new hardware and/or to divest the old hardware units is made on average every two months ($I^{I-D} = 60$ days). This mechanism is implemented as in [13]. Note that for each sell market order issued by miners, the system generates automatically a buy order, giving to the miners the corresponding fiat cash since the model does not include the presence of other kinds of agents, hence the presence of buy orders.

3.1.2. Second Strategy: Adjusting the Hashing Capability as a Function of the Bitcoin Price Trend

We assumed that miners, operating in the market, adjust their economic balance turning on or turning off some of their mining hardware units, in order to adjust their electricity consumption and their maintenance expenses. The decision of turning on/off their mining hardware units is made by evaluating the relative strength index, a technical analysis indicator that gives overbought and oversold signals.

Specifically, the percentage of hashing capability to turn on/off, $\gamma^{off/on}$, is equal to a random variable characterized by a lognormal distribution with an average of 0.6 and a standard deviation of 0.15. If $\gamma^{off/on} > 1$, it is set equal to one. The overbought signal is given when the RSI (Relative Strength Index)value is over a specific benchmark (comprised between 70 and 80), and the oversold signal is given when this value is under another benchmark (comprised between 20 and 30). Hence, if the evaluation results in an oversold signal, miners expect a price increase and consequently turn on the machines previously turned off. The other way around, if the evaluation results in an overbought signal, miners expect a price decrease and consequently turn off the machines previously turned on.

The decision to operate on their hashing power or not is made by every mining pool from time to time, on average every 10 days ($I^{off/on} = 10$) following a mechanism similar to that to decide whether to buy new hardware and divest old units.

If the i^{th} miner decides whether to turn off/on hardware units at time t, the next time, $t_i^{turnOff/On}(t)$, she/he will decide again is given by Equation (5):

$$t_i^{off/on}(t) = t + int(I^{off/on} + N(\mu^{off/on}, \sigma^{off/on})) \quad (5)$$

where int rounds to the nearest integer and $N(\mu^{off/on}, \sigma^{off/on})$ is a normal distribution with average $\mu^{off/on} = 0$ and standard deviation $\sigma^{off/on} = 2$. $t_i^{off/on}(t)$ is updated each time the miner makes her/his decision.

3.2. Simulation Results

The models just described were implemented in Smalltalk language and run in the period between 1 January 2017 and 31 May 2018, hence over a simulation period equal to 513 steps, each simulation step being equal to one day. Note that we sized the artificial market at about 1/100 of the real

market, to be able to manage the computational load of the simulation; for this reason, we divided the number of miners and that of Bitcoins by 100. For the model's calibration, we refer to [13], if not otherwise specified.

3.2.1. Total Wealth Per Capita and Hash Rate

At first, we analyzed the total average wealth per capita of miners. Figure 1 shows the comparison of the total average wealth per capita of the miner population, both when miners apply only the first miner's strategy and when they apply both proposed miners' strategies, assuming γ_1 and $\gamma^{off/on}$ equal to 0.5. Remember that γ_1 is the percentage of cash invested to buy new hardware and $\gamma^{off/on}$ is the percentage of hashing capability to turn on/off. The figure highlights that miners, which adopt both miners' strategies proposed (hence, they buy new hardware units, divest old hardware units, and adjust their hashing capability, following the mechanism described in Section 3.1), are able to achieve profits higher over time than miners that adopt only the first strategy, hence those who buy new hardware units and divest the old hardware units.

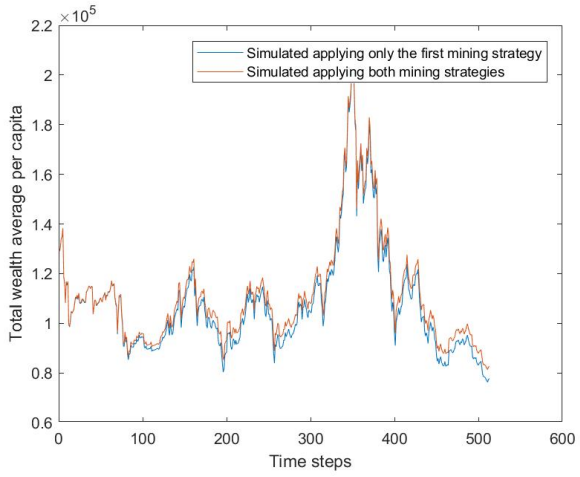

Figure 1. Comparison of the total average wealth per capita of the miner population, both when miners apply only the first proposed strategy and when they apply both proposed strategies, in the market using the Proof of Work (PoW).

We studied the sensitivity of the model to the parameters γ_1 and $\gamma^{off/on}$. We varied the average percentage of the wealth that miners allocate for buying new hardware, γ_1, to verify how varying this parameter can impact miners' success.

Figure 2a shows the average and the standard deviation (error bars) of the total wealth per capita for miners, at the end of the simulation period, for increasing values of γ_1. The average of the values reported in the figure is equal to $Q = 1.16 \times 10^8$. We set γ_1 to 0.5, because the average total wealth per capita associated with this value of γ_1 is close to Q and the standard deviation of the total wealth per capita is low. Figure 2b shows the average and the standard deviation (error bars) of the total wealth per capita for miners, at the end of the simulation period, for increasing values of the average of $\gamma^{off/on}$, having set γ_1 to 0.5. We set $I^{off/on} = 10$, because the values of profits do not vary much with $I^{off/on}$, and $\gamma^{off/on}$ to 0.5, because 0.5 is the lower value of $\gamma^{off/on}$ that allows miners who adopt both strategies to achieve higher profit over all simulation periods than the profits obtained by miners who adopt only the first strategy.

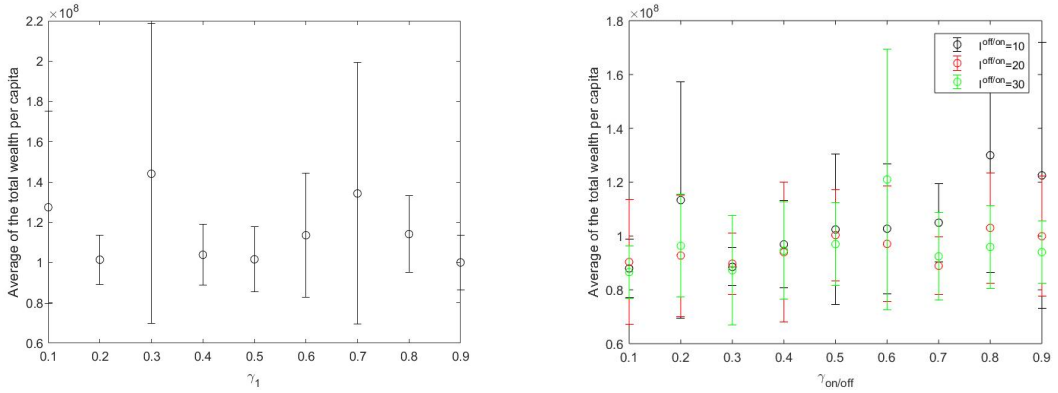

Figure 2. Average and error bar (standard deviation) of the total wealth per capita for miners at the end of the simulation period, across all Monte Carlo simulations for increasing values of the average of γ_1 in a market using only the first miners' strategy (**a**,**b**) of $\gamma^{off/on}$ in a market using both miners' strategies while $I^{off/on}$ varies acquiring three values, 10, 20, or 30.

Figure 3 shows the comparison of the simulated and real hash rate, both when miners adopt only the first miners' strategy and when they adopt both miners' strategies. Results show that by applying both miners' strategies, the system can better reproduce the real hash rate trend, introducing a fluctuating trend. Note that the simulated quantities in figure have been multiplied by 100, which is the resizing applied to the real market.

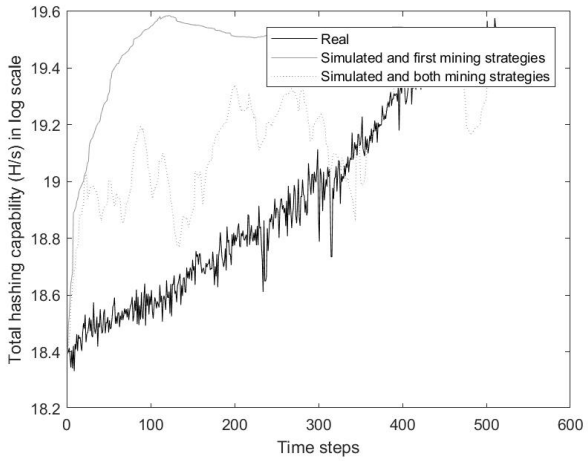

Figure 3. Comparison of the simulated and real hash rate, both when miners adopt only the first strategy and when they adopt both proposed miners' strategies.

3.2.2. Total Power Consumption and Total Cost per Mined Bitcoin

Figure 4a describes the average and standard deviation of the power consumption in Watts across all Monte Carlo simulations. Its order of magnitude is about 10^{10} considering our market resizing. This power consumption refers to the total consumption of power needed to supply the mining hardware units.

Figure 4b describes the average and standard deviation of the total expenses, including the expenses needed to set up and maintain the mines, across all Monte Carlo simulations.

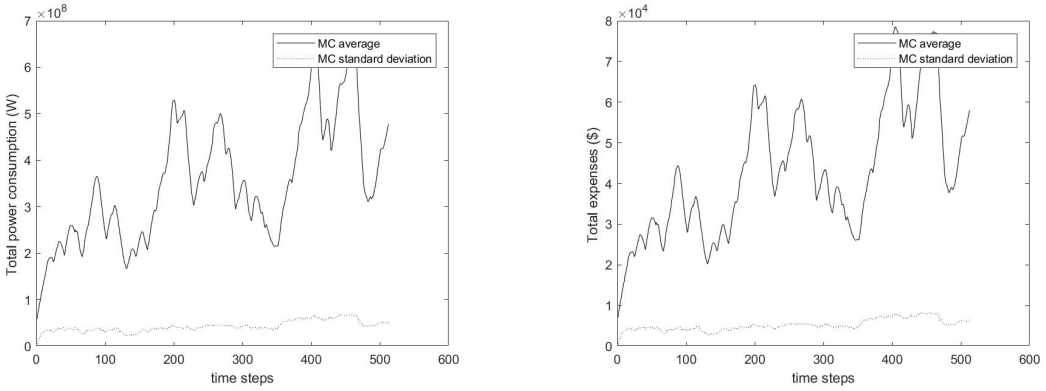

Figure 4. Average and standard deviation (**a**) of the power consumption expressed in Watts to power the mining hardware units and (**b**) of the total expenses expressed in dollars, including the expenses needed to set up and maintain the mines, across all Monte Carlo simulations in the market using PoW.

Once having computed the total electricity expenses and the costs to set up and maintain the mines, we computed as a result the average and standard deviation of the total mining cost per mined Bitcoin expressed in dollars across all Monte Carlo simulations (see Figure 5). This cost varies over time, and its average value is equal to $2.376. This value, which is computed taking into account the electricity costs in Sichuan, a province in southwest China (see Footnote 5), is not too far from that described in a recent article that estimated the cost per mined Bitcoin as equal to $3.172 in China [28].

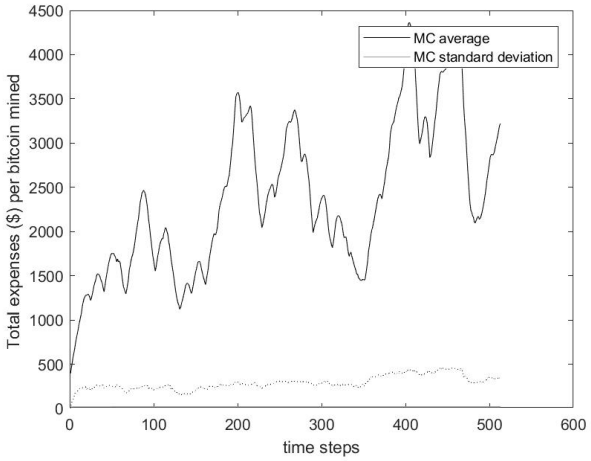

Figure 5. Average and standard deviation of the total mining cost per mined Bitcoin expressed in dollars across all Monte Carlo simulations.

3.3. Total Power Consumption in a Hypothetical Bitcoin System Using PoS

In the following, we computed the total power consumption in a hypothetical Bitcoin system using PoS as a consensus mechanism. This mechanism is implemented as in the Nxtsystem, which is a 100% PoS cryptocurrency system that is less popular than Bitcoin (see [29,30]).

In the real Bitcoin network, the miners have to run their mining hardware continually in order to secure the network. Contrary to Bitcoin, in the Nxt system, everyone who owns Nxt can be chosen to protect the network. The probability to be chosen is proportional to the Nxt owned. With this mechanism, the computers run to validate the transactions and not to secure the network.

In general, in a cryptocurrency market using PoS, everyone holding an amount $b_i(t)$ of Bitcoins has a probability higher than zero of mining Bitcoins. This probability is proportional to the cryptocurrency owned by the i^{th} user, b_i [30].

Everyone holding Bitcoins can be a potential miner, but replicating the work by Czarnek [31], we hypothesized that the validation of a block involves a number of miners (In the Nxt system, people creating blocks are called "forgers". This stems from the name of the process of block generation known as "forging".) equal to three, which are in the full power state while forging (in [31], the author assumed three forgers and not only on,e because multiple forgers, operating at the same time, keep each other honest and increase the network security).

Note that miners do not belong to a pool. This is because, in a system based on PoS, there is no arms race for acquiring specialized hardware needed to run computations, and hence, there is no need to pool together to share resources. PoS is CPU friendly; consequently, we assumed that each miner owns a machine characterized by a power consumption equal to 130 W while she/he mines.

The power consumption in the hypothetical system is computed simply taking into account the power consumption of the mining machines. Assuming that the potentialities of the mining hardware do not vary in the simulation period and fixing the number of machines involved in the mining activity of a block equal to three, the machine power consumption per hour equals 130 W; the time needed to validate a block equals ten minutes; and the number of blocks per day is equal to 144; it follows that the power consumption per day is constant and equal to:

$$\frac{130\ W}{6} \times 3 \times 144 = 9360\ W.$$

Thus, the cost per mined Bitcoin is equal to $\$0.442 \times 10^{-3}$, the number of Bitcoin per block being equal to 12.5. Of course, the cost per mined Bitcoin is lower in this PoS system than that estimated for the system using PoW.

4. Conclusions

In this work, we presented an overview of the gold mining industry and a model to simulate the Bitcoin mining activity. To analyze the gold mining industry, we examined the lifecycle of the gold, which comprises several stages to take the metal ore from the Earth and convert it into gold bullion. All these stages require large investments, but also much time, and given that gold is becoming both harder to mine and more scarce, these stages are going to become increasingly expensive.

In order to analyze the Bitcoin mining activity, we presented an agent-based artificial market model that simulates this mining activity.

The simulation results show the ability of the model to reproduce the total hash rate in the real Bitcoin market and how miners are able to get a higher total wealth per capita by adjusting the expenses by turning off/on a fraction of the mining hardware units. The results allow us to compute the total expenses sustained by miners and the potential savings of a hypothetical Bitcoin system under PoS with respect to the simulated Bitcoin system that uses PoW, as does the real one.

Gold and Bitcoin have much in common, in terms of rarity, scarcity and transportability. With respect to the overall infrastructure, Bitcoin could be considered superior to gold and also, in general, to traditional financial systems. This work highlights that a cryptocurrency system, in order to work, requires an infrastructure much leaner than that of the gold system and also leaner than that of the traditional financial systems. Contrary to cryptocurrency systems, in general, a traditional financial system requires much time and money to invest in infrastructure, in electricity, in gas and water consumed by employees, and in management of the waste produced. In addition, all fiat currencies imply a cost for their creation and also a maintenance cost to guarantee the quality standards for the banknotes in circulation over time. All these costs are missing in a cryptocurrency system.

In the last ten years, many cryptocurrency systems have been created. Cryptocurrencies are a means of accounting and storing value, but also are a global peer-to-peer means of payment.

Today cryptocurrencies are used also as a means for raising capital, and there are many systems that manage smart contracts, which is computer code that automatically executes an agreement (triggers a claim) when a given event occurs via blockchain technology. Ten years ago, all this was unthinkable.

Due to the potentialities of the cryptocurrencies and their underlying technology, we would not be surprised if blockchain technology were able to support or replace national money and traditional means of payment in a future not too far from now.

Author Contributions: Conceptualization: L.C. and M.M.; Methodology: L.C.; Software: L.C.; Validation: L.C.; Formal Analysis: L.C.; Writing-Original Draft Preparation: L.C.; Writing-Review & Editing: L.C. and R.T.; Supervision: R.T. and M.M.

Funding: This research is partially supported by the research project Fondazione di Sardegna "Algorithms for Approximation with Applications [Acube]", annuity 2017; and by the research project "AIND-Amministrazioni e Imprese Native Digitali"-Programmazione Unitaria 2007-2013-P.O. (Programma Operativo)FESR (Fondo Europeo di Sviluppo Regionale)2007/2013-Interventi a sostegno della competitivitá e dell'innovazione, annuity 2013.

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

References

1. Young, J. Proof of Work vs Proof of Stake: Merits and Disadvantages. 2016. Available online: http://www.coinfox.info/news/reviews/6417-proof-of-work-vs-proof-ofstake-merits-and-disadvantages (accessed on 15 June 2018).
2. Cointelegraph.com. The Inevitable Failure of Proof-of-Stake blockchains and Why a New Algorithm is Needed (Op-Ed). 2015. Available online: https://cointelegraph.com/news/the-inevitablefailure-of-proof-of-stake-blockchains-and-why-a-new-algorithmis-needed (accessed on 15 June 2018).
3. Akhtar. Is Bitcoin the New Gold? 2017. Available online: https://www.thestreet.com/story/14285619/1/is-Bitcoin-stealing-gold-s-safe-haven-status.html (accessed on 15 June 2018).
4. Cocco, L.; Pinna, A.; Marchesi, M. Banking on blockchain: Costs Savings Thanks to the blockchain Technology. *Future Int.* **2017**, *9*, 25. [CrossRef]
5. McLean, J. Banking on bLockchain: Charting the Progress of Distributed Ledger Technology in Financial Services. 2016. Available online: https://www.ingwb.com/media/1609652/banking-on-blockchain.pdf (accessed on 15 June 2018).
6. Bradley. The Energy Efficiency Bitcoin. 2016. Available online: https://www.cryptocoinsnews.com/energy-efficiency-Bitcoin/ (accessed on 15 June 2018).
7. McCook, H. Under the Microscope: The True Costs of Gold Production. 2014. Available online: https://www.coindesk.com/microscope-true-costs-gold-production (accessed on 15 June 2018).
8. Rajaee, M.; Sınchez, B.N.; Renne, E.P.; Basu, N. An Investigation of Organic and Inorganic Mercury Exposure and Blood Pressure in a Small-Scale Gold Mining Community in Ghana. *Int. J. Environ. Res. Public Health* **2015**, *12*, 10020–10038. [CrossRef] [PubMed]
9. Schutzmeier, P.; Berger, U.; Bose-O'Reilly, S. Gold Mining in Ecuador: A Cross-Sectional Assessment of Mercury in Urine and Medical Symptoms in Miners from Portovelo/Zaruma. *Int. J. Environ. Res. Public Health* **2017**, *14*, 34. [CrossRef] [PubMed]
10. Asamoah, E.F.; Zhang, L.; Liu, G.; Owusu-Prempeh, N.; Rukundo, E. Estimating the "Forgone" ESVs for Small-Scale Gold Mining Using Historical Image Data. *Sustainability* **2017**, *9*, 1976. [CrossRef]
11. Mihai, A.; Marincea, A.; Ekenberg, L. A MCDM Analysis of the Rosia Montana; Gold Mining Project. *Sustainability* **2015**, *7*, 7261–7288. [CrossRef]
12. Rajaee, M.; Long, R.N.; Renne, E.P.; Basu, N. Mercury Exposure Assessment and Spatial Distribution in A Ghanaian Small-Scale Gold Mining Community. *Int. J. Environ. Res. Public Health* **2015**, *12*, 10755–10782. [CrossRef] [PubMed]
13. Cocco, L.; Marchesi, M. Modeling and Simulation of the Economics of Mining in the Bitcoin Market. *PLoS ONE* **2016**, *11*, e0164603. [CrossRef] [PubMed]
14. Writer, S. The 5 Stages of the Mining Life Cycle. 2015. Available online: http://www.miningglobal.com/operations/gifs-5-stages-mining-life-cycle (accessed on 15 June 2018).
15. Fulp, M. The Real Cost of Mining Gold. 2015. Available online: http://www.kitco.com/ind/fulp/2015-02-04-The-Real-Cost-of-Mining-Gold.html (accessed on 15 June 2018).

16. Koven, P. Exactly How Much Does It Cost to Produce an Ounce of Gold? 2014. Available online: https://business.financialpost.com/commodities/mining/exactly-how-much-does-it-cost-to-produce-an-ounce-of-gold (accessed on 15 June 2018).
17. providentmetals.com. How Much Does it Cost to Produce an Ounce of Gold? 2017. Available online: https://blog.providentmetals.com/facts-and-history/how-much-does-it-cost-to-produce-an-ounce-of-gold.htm#.W50Zz_ZuIcQ (accessed on 15 June 2018).
18. srsroccoreport.com. Top Gold Miners Burned Record Amount Of Fuel To Produce Gold in 2015. 2016. Available online: https://srsroccoreport.com/top-gold-miners-burned-record-amount-of-fuel-to-produce-gold-in-2015/ (accessed on 15 June 2018).
19. Anonymous. How Many People Touched Bitcoin up to 2017 and What Is the Current Adoption Pace? 2017. Available online: https://steemit.com/Bitcoin/@jimmco/how-many-people-touched-Bitcoin-up-to-2017-and-what-is-current-adoption (accessed on 15 June 2018).
20. Pinna, A.; Tonelli, R.; Orrú, M.; Marchesi, M. Petri Nets Model for Blockchain Analysis. *Comput. J.* **2018**, *61*, 1374–1388. [CrossRef]
21. Gibrat, R. *Les in'egalit'es 'economiques*; Librairie du Recuil Sirey: Paris, France, 1931.
22. Yule, G. A mathematical theory of evolution based on the conclusions of Dr. J.C. Willis. *Philos. Trans. B CCXIII* **1924**, *213*, 21–87. [CrossRef]
23. newsChina. Bitcoin Miners. 2017. Available online: http://newschinamag.com/newschina/articleDetail.do?article_id=2348 (accessed on 15 June 2018).
24. aljazeera.com. Inside the World of Chinese Bitcoin Mining. 2018. Available online: http://www.chinafile.com/multimedia/photo-gallery/inside-world-of-chinese-Bitcoinmining (accessed on 15 June 2018).
25. Tuwiner, J. Bitcoin Mining in China. 2017. Available online: https://www.buyBitcoinworldwide.com/mining/china/ (accessed on 15 June 2018).
26. Vincent, D. We Looked Inside Asecret Chinese Bitcoin Mine. 2016. Available online: http://www.bbc.com/future/story/20160504-we-looked-inside-a-secret-chineseBitcoin-mine (accessed on 15 June 2018).
27. Tan, W. Brief Overview of China's Cryptocurrency Mining: Capital, Costs, Earnings. 2017. Available online: https://cointelegraph.com/news/brief-overview-of-chinas-cryptocurrencymining-capital-costs-earnings (accessed on 15 June 2018).
28. trustnodes.com. Bitcoin Mining Costs Just $3,000 in China, $500 in Venezuela, $4,700 in USA. 2018. Available online: https://www.trustnodes.com/2018/04/26/Bitcoin-mining-costs-just-3000-china-500-venezuela-4700-usa (accessed on 15 June 2018).
29. Nxt Community. Nxt Whitepaper. 2014. Available online: https://bravenewcoin.com/assets/Whitepapers/NxtWhitepaper-v122-rev4.pdf (accessed on 15 June 2018).
30. Nxt. The Math of Nxt Forging. 2014. Available online: https://www.docdroid.net/abp9/forging0-3-1.pdf (accessed on 15 June 2018).
31. Czarnek, M. Nxt Network Energy and Cost Efficiency Analysis. 2014. Available online: https://www.scribd.com/document/254930279/Network-Energy-and-Cost-Efficiency-Analysis (accessed on 16 January 2017).