An agent based model to analyse the Bitcoin Mining Activity and a Comparison with Gold Mining Industry

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

1 Department of Electric and Electronic Engineering, University of Cagliari, Cagliari 09123, Italy
2 Department of Mathematics and Computer Science, University of Cagliari, Cagliari 09124, Italy
* Correspondence: luisanna.cocco@diee.unica.it

Abstract: In this paper, we present an interesting analysis about the mining process of two popular assets, bitcoin and gold. The analysis highlights as bitcoin, specifically its underlying technology, allows facing the modern environmental challenges better than gold. In addition it emphasizes as 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 to conduct to produce an ounce of gold, and an artificial agent-based market model that simulates the bitcoin mining process allowing to quantify the bitcoin mining costs. In this market model miners validate the bitcoin transactions using the Proof of Work as consensus mechanism, get a reward in bitcoins, sell a fraction of them to cover their expenses, and stay competitive in the market 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, that are distributed databases that bundle the transactions into blocks. Cryptocurrencies’ 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 that have to be created in such a way to be very, very hard to cheat.

In 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 dominance and due to 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 a long-term sustainability. Others are convinced that a system using PoS as consensus mechanism creates a problem of monopoly1. In

---

1 Refer to the article by Young [29].
a PoW network, all 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 centralisation 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 basic algorithm and offer additional security assigning the voting power according to precise "target value" depending 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 article by Cointelegraph.com [8]).

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 [1]). In terms of rarity and scarcity, transportability and above all infrastructure, maybe 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 will be reached no bitcoin will be generate anymore. Contrary bitcoin, the availability of gold depends on the supply-and-demand cycles, and a high demand for gold gives incentive for the gold miners to find mine more.

As regards transportability–that refers to how easy it is to move from one location to another them to complete an exchange– the transportability of bitcoin is higher than gold bullion because it is transportable like a digital file.

As regards infrastructure–that refers to the whole system that generates and distributes an asset– in the actual Bitcoin system, in order to produce bitcoin we have 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 math 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 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 we have move through several stages. It is necessary discovering where the gold deposits may be, analysing 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, infrastructure must be constructed then 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, to take the metal ore from the earth and converting it to gold bullion, are quite expensive. In addition they are becoming more and more expensive given gold is becoming both harder to mine and more scarce.

Looking at a sustainable development, bitcoin mining infrastructure allows to better address the environmental aspects of sustainability and given the high interest in this technology, in the near future could have a Bitcoin protocol ecologically friendly that allows to reduce the mining cost, hence to have a system that allows to save money and reduce the carbon footprint (see [7]). In addition, Blockchain technology has the ability to promote economic growth because it allows the free trade that speeds the technological innovation, leading also to the development of green technologies (see work by McLean [14]). The introduction of this 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 (see [5]).

Contrary Bitcoin, the carbon footprint of gold will continue to increase, given most of the energy used in mining comes from non-renewable fossil fuels like diesel, that hardly is replaceable with renewable resources (see [13]). In addition gold industry has caused environmental and health
problems for decades for 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 [21,22].

So, looking at total mining costs, such as production costs, economic costs, environmental costs, and social costs, of these two assets probably a wide spread of bitcoin could allow us to better address the environmental aspects of sustainability and to have substantially higher savings than gold2 ([4,15,20–22]).

In this paper, we present an analysis of the gold mining process, and proposed 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. [6].

The agents present in the market are the Miners that validate the bitcoin transactions, get a reward in Bitcoin, and sell a fraction of their mined bitcoin to cover their expenses. They stay competitive in the market by 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, that 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 the Bitcoin network is performing – and compute the total expenses sustained by miners, showing as 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 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 consensus mechanism, and in a hypothetical Bitcoin system using 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, analysing the promising areas and performing drill testing are the activities made in these stages. To pin out potential deposits of gold the companies engage geologists and others competent figure. 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 is collected, we can move 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 the identified area a mining activity worthwhile is associated, the construction stage takes place, and infrastructure is built. This stage involves building roads, processing facilities, environmental management systems, employee housing and other facilities. It can take long time, up to 5 years between the times in which the promising area is discovered and the time in which actual mining activity takes place.

Built infrastructure we arrive at the production stage. 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, technology, environmental and economical concerns (see [28]). 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 a processing on-site 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.

After production stage we move forward the final stages. When the mining site has been exhausted, closing the site and dismantling all facilities on the property is necessary. 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 [28]).

As you can see, extracting metal ore from the earth and converting it to gold bullion is quite extensive and requires a lot front-end investment and time.

According to experts the reporting of the gold industry’s cost is unclear, and probably the really costs to produce an ounce of gold does not clearly described yet. Let us start looking into the history of gold cost reporting in the industry (see [10,12]).

In the mid-1990s, the industry introduced “cash costs” to shed light on the gold industry’s cost, and shed the reputation that 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). So, 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, that becomes bigger and bigger as mines get older and grades decline, and the G&A expenses but it does not include costs such as project capital or dividends.

In an article published by providentmetals.com [19] the author wrote that the gold mining costs were underestimated until the 1990s. In those years the values of these costs fluctuated between the $500 and the $800 per ounce and do not consider for example the expenses to buy and repair the equipments and those to run the whole company. After the introduction of the AISC metric these costs increase. They are estimated over $1,000 per ounce (see works [19], and [13]) 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 are expected to increase since most of the energy used in mining comes from non-renewable fossil fuels (see [13]). In 2005, Barrick and Newmont, two of the world’s largest gold producer, 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 (ref. [23]).


The model presented in this work is a modified version of the model proposed in the work by Cocco et al. [6]. 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 to each time \( t \), the number of miners is constant over time\(^4\) and the bitcoin price is an exogenous variable.

\(^3\) The number of Bitcoins \( b_i \) mined by \( i \)-th pool per day is computed easily Knowing the number of blocks discovered per day, and consequently knowing the number of new Bitcoins \( B \) to be mined per day. Refer to work [6] for more details.

\(^4\) 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 [6]). This number is computed following the approach proposed [6], in which the authors assumed that in the early days of Bitcoin system these people were the people who trade bitcoins,
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 US dollars, and a precise crypto cash, \( b_i(0) \) expressed in bitcoins, where \( i \) is the trader’s index\(^5\).

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 initial of the simulation. Known this value we distributed it among the miners in proportional way to their wealth (ref. [11,30]). 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 \( r_i(0) \), that 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 analysed the bitcoin mining costs from January 1st, 2017 to May 31st, 2018 the assumptions above are reasonable.

Note that we considered the electricity expenses equal to 70 percent of the total bitcoin mine’s expenses (ref. [2,16]) and as a result, known 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 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 \( i-th \) trader at time \( t \), \( r_i(t) \) expressed in \([H/sec]\), and the total electricity cost \( e_i(t) \) expressed in \$ per day, associated to her mining hardware units, are defined as in work [6] respectively as:

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

and

\[
 e_i(t) = \sum_{s=t^E}^{t} c * P * r_{i,u}(s) * 24 \tag{2}
\]

where:

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

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

Let us describe the variables in the equation above, briefly (for more details refer to work by Cocco et al. [6]). \( R \) is the hash rate which can be bought with one US$, expressed in \( \frac{H}{sec} \), and \( P \) is the power consumption, expressed in \( \frac{W}{sec} \). Since we assumed that in future no technological breakthrough occurs we assumed that Antminer S9 is the only mining hardware machine in our artificial market.

So the value of hash rate, \( R \), is fixed to \( 5.833 \times 10^9 \frac{H}{sec} \), and the power consumption, \( P \), is fixed to

---

\(^5\) The wealth distribution, both in crypto and fiat cash, of miners follows a Zipf law (see work [6] for more details).
0.099/10^9 \frac{W}{\text{unit}}. The number 24 represent the total hours in a day. \( r_{i,u}(t) \) is the hashing capability of
the hardware units \( u \) bought at time \( t \) by \( i-th \) miner, and \( \gamma_1 \) and \( \gamma_1 \) 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. \( c \) is the fiat price per Watt and per hour. It is assumed equal to 8.5 * 10^{-5 } \$, considering the cost of 1 KWh equal to 0.085$.

Every miner buys new hardware units, if their 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
taken on average every two months (\( t^{1-D} = 60 \text{ days} \)). This mechanism is implemented as in work by
[6], refer to this work for more detail. 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 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, and their
maintenance expenses. The decision of turning on/off their mining hardware units is taken 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, \( \gamma_{on/off} \), is equal to a random
variable characterized by a lognormal distribution with average 0.6 and standard deviation 0.15. If
\( \gamma_{on/off} > 1 \) if it sets equal to one. The overbought signal is given when the RSI value is over a
specific benchmark (comprises between 70 and 80) and the oversold signal is given when this value
is under another benchmark (comprises 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. Vice versa, 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 taken by each mining pool from time to
time, on average every 10 days (\( t^{10} = 10 \) following a mechanism similar to that to decide whether
to buy new hardware and divest old units.

If \( i-th \) miner decides whether to turn off/on hardware units at time \( t \), the next time,
\( t_{i}^{\text{turnOff/On}}(t) \), she will decide again is given by eq. 5:

\[
t_{i}^{\text{turnOff/On}}(t) = t + \text{int}(\gamma_{on/off} + N(\mu_{on/off}, \sigma_{on/off}))
\]

where int rounds to the nearest integer and \( N(\mu_{on/off}, \sigma_{on/off}) \) is a normal distribution with
average \( \gamma_{on/off} = 0 \) and standard deviation \( \sigma_{on/off} = 2 \). \( t_{i}^{\text{turnOff/On}}(t) \) is updated each time the miner
takes her decision.

3.2. Simulation Results

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

\[\text{The fiat price per Watt and per hour refers to the electricity cost in Sichuan. This is because, today Chinese mining pools control more than 70% of the Bitcoin network’s collective hashrate (ref. [26,27]). China is the undisputed world leader in Bitcoin mining: it manufactures most of the world’s mining equipment, massive mining farms are located in China as its electricity tariff is one of the lowest in the world. The largest concentration of miners are located in Sichuan, a province in southwest China, estimated to be about 30 percent of the total. Electricity in Sichuan costs around $0.08 to $0.09/KWh for commercial and industrial consumption (ref. [24]). To benefit of a low electricity tariff is extremely important because electricity typically accounts for 60-70 percent of a bitcoin mine’s expenses (ref. [2,16]). In addition the Chinese exchanges used to lead the world in terms of volume – Antpool is Chinese based mining pool, maintained by Bitmain, a ASIC manufacturer.}\]
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 refers to the work [6], if not otherwise specified.

3.2.1. Total wealth per capita and hash rate

At first we analysed the total average wealth per capita of miners. Fig. 1 shows the comparison of the total average wealth per capita of miner population, both when miners apply only the first miners strategy and when they apply both the proposed miners strategies, assuming $\gamma_1$ and $\gamma_{\text{off/on}}$ equal to 0.5. Remember that $\gamma_1$ is the percentage of cash to buy new hardware and $\gamma_{\text{off/on}}$ is the percentage of hashing capability to turn on/off. The figure highlights as Miners, that adopt both the 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 profit higher over time than Miners that adopt only the first strategy, hence that buy new hardware units and divest the old hardware units.

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

![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 $\gamma_1$ in a market using only the first miners strategy (a) and (b) of $\gamma_{\text{off/on}}$ in a market using both the miners strategies while $\text{l}_{\text{off/on}}$ varies acquiring three values 10, 20 or 30.](image)
We studied the sensitivity of the model to the parameters $\gamma_1$ and $\gamma_{\text{off/on}}$. We varied the average percentage of the wealth that Miners allocate for buying new hardware, $\gamma_1$, to verify how varying this parameter can impact on Miners’ success.

Fig. 2 (a) 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 $\gamma_1$. The average of the values reported in figure is equal to $Q = 1.16 \times 10^8$. We set $\gamma_1$ to 0.5, because the average total wealth per capita associated to this value of $\gamma_1$ is close to $Q$ and the standard deviation of the total wealth per capita is low. Fig. 2 (b) 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 $\gamma_{\text{off/on}}$, having set $\gamma_1$ to 0.5. We set $I_{\text{off/on}} = 10$ because values of profits do not vary much with $I_{\text{off/on}}$, and $\gamma_{\text{off/on}}$ to 0.5 because 0.5 is the lower value of $\gamma_{\text{off/on}}$ that allows miners who adopt both the strategies to achieve higher profit over all simulation period than the profits gotten by miners who adopt only the first strategy.

Fig. 3 shows the comparison of the simulated and real hash rate, both when miners adopting only the first miners’ strategy and when they adopt both the miners’ strategies. Results show that applying both the miners’ strategies the system can reproduce better the real hash rate trend introducing a fluctuating trend. Note that the simulated quantities in figure have been multiplied for 100 that is the resize 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 the proposed miners’ strategies.

3.2.2. Total Power Consumption and total cost per mined bitcoin.

Fig. 4 (a) describes the average and standard deviation of the power consumption in Watt across all Monte Carlo simulations. Its magnitude order is equal to $10^{10}$ considering our market resize. This power consumption refers to the total consumption of power needed to power the mining hardware units.

Fig. 4 (b) 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. Once 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 fig. 5). This cost varies over time and its average value is equal $2.376. This value, that is computed taking into account the electricity costs in Sichuan a province in southwest China (see footnote 5), is not too far by that described in a recent article that estimates the cost per mined bitcoin equal to $3.172 in China [25].
Figure 4. Average and standard deviation (a) of the power consumption expressed in Watt 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 market using PoW.

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 Nxt system, that is a 100% PoS cryptocurrency system less popular than Bitcoin system (see works [17] and [18]).

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 every one 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 every one, holding an amount $b_i(t)$ of bitcoins, has a probability higher than 0 to mine bitcoins. This probability is proportional to the cryptocurrency owned by the user $i - th$, $b_i$ (ref. [18]).
Every one holding bitcoins can be potential miners, but as in work by Czarnek [9] we hypothesized that the validation of a block involves a number of miners equal to three, that are in full power state while forging\(^8\).

Note that miners do not belong to a pool. This is because, in a system based on PoS there is not an arms race for acquiring specialized hardware needed to run computations, and hence there is not a necessity 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 130W while she/he mines.

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

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

Follows that the cost per mined bitcoin is equal to $0.442 \times 10^{-3}$ being the number of bitcoin per block 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 present an overview of the gold mining industry and a model to simulate the bitcoin mining activity. To analyse the gold mining industry we present the lifecycle of the gold, that comprises several stages to take the metal ore from the earth and converting it to gold bullion. All these stages require large investments but also much time and given gold is becoming both harder to mine and more scarce these stages are going to become increasingly expensive.

Instead to analyse the bitcoin mining activity we present an agent based artificial market model that simulates this mining activity.

Simulation results show the ability of the model to reproduce the total hash rate in the real Bitcoin market, and as 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. 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 and in terms of rarity and scarcity, transportability and above all infrastructure, maybe bitcoin could be considered superior to gold, and also in general to traditional financial systems. This work highlights as a cryptocurrency system requires to work an infrastructure much leaner than that of the gold system but also than the traditional financial systems. Contrary to cryptocurrencies’ systems, in general a traditional financial system requires much time and much 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 not present in a cryptocurrency system.

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

---

\(^7\) In the Nxt system people creating blocks are called "forgers", this stems from the name of the process of block generation known as "forging".

\(^8\) In [9] the author assume three forgers and not only one because multiple forgers, operating at the same time, keep each other honest and increase the network security.
cryptocurrencies are used also as mean for raising capital and many are the systems that manage smart contracts, that is computer code that executes automatically an agreement (triggers a claim) when a given event occurs via Blockchain technology. Ten years ago all this was unthinkable.

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


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

References


© 2018 by the authors. Submitted to Journal Not Specified for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).