



# The Cost of Bitcoin Mining Has Never Really Increased

Yo-Der Song<sup>1,2</sup> and Tomaso Aste<sup>1,2\*</sup>

<sup>1</sup> Department of Computer Science, University College London, London, United Kingdom, <sup>2</sup> UCL Centre for Blockchain Technologies, University College London, London, United Kingdom

## OPEN ACCESS

### Edited by:

Joerg Osterrieder,  
Zurich University of Applied Sciences,  
Switzerland

### Reviewed by:

Daniel Traian Pele,  
Bucharest Academy of Economic  
Studies, Romania  
Luca Di Persio,  
University of Verona, Italy  
Dagmar Linnertova,  
Masaryk University, Czechia  
Eftim Zdravevski,  
Saints Cyril and Methodius University  
of Skopje, North Macedonia  
Dave Remue,  
KPMG, Belgium

### \*Correspondence:

Tomaso Aste  
t.aste@ucl.ac.uk

### Specialty section:

This article was submitted to  
Financial Blockchain,  
a section of the journal  
Frontiers in Blockchain

**Received:** 25 May 2020

**Accepted:** 31 August 2020

**Published:** 22 October 2020

### Citation:

Song Y-D and Aste T (2020) The Cost  
of Bitcoin Mining Has Never  
Really Increased.  
*Front. Blockchain* 3:565497.  
doi: 10.3389/fbloc.2020.565497

The Bitcoin network is burning a large amount of energy for mining. In this paper, we estimate the lower bound for the global mining energy cost for a period of 10 years from 2010 to 2020, taking into account changes in energy costs, improvements in hashing technologies and hashing activity. We estimate energy cost for Bitcoin mining using two methods: Brent Crude oil prices as a global standard and regional industrial electricity prices weighted by the share of hashing activity. Despite a 10-billion-fold increase in hashing activity and a 10-million-fold increase in total energy consumption, we find the cost relative to the volume of transactions has not increased nor decreased since 2010. This is consistent with the perspective that, in order to keep the Blockchain system secure from double spending attacks, the proof of work must cost a sizable fraction of the value that can be transferred through the network. We estimate that in the Bitcoin network this fraction is of the order of 1%.

**Keywords:** bitcoin, proof of work, cryptocurrency, blockchain, mining cost

## 1. INTRODUCTION

Bitcoin is a digital currency launched in 2009 by an anonymous inventor or group of inventors under the alias of Satoshi Nakamoto (Nakamoto, 2019). It is the largest cryptocurrency in market capitalization with over 100 billion dollars (Chan et al., 2019; Grobys and Sapkota, 2019; Blockchain.com, 2020). As a decentralized currency, Bitcoin differs from government regulated fiat currencies in that there exists no central authority within the network to verify transactions and prevent frauds and attacks (Sin and Wang, 2017). Instead, Bitcoin relies on a highly replicated public ledger, secured by means of a hash chain and validated through community consensus (Akcora et al., 2018). All users can announce a new transaction but such a transaction will be considered valid and included in the ledger only once it is verified by a majority of the network nodes. Transactions are written into blocks that are interlocked into a chain by hashes. Hashing is a one-way function that maps an input of arbitrary length into a string of a fixed number of digits. The hash function must guarantee that the output string is (quasi-)uniquely related to the given input (deterministic) and that small changes in the input should cause arbitrarily large changes in the output so that reconstructing the input based on the output is infeasible. In the case of Bitcoin, the transactions in the new proposed block and the header of the most recent block is inputted into the SHA-256 hash algorithm, making therefore a chain with unique direction. Such a chain is at the heart of the Bitcoin security because it makes it difficult to alter the content of a block once subsequent blocks are added to the chain. In Bitcoin, this cryptographic sealing process through a hash chain is intentionally designed to be computationally intensive by accepting hashes only if the randomly generated hash number is smaller than a given target. Therefore the community performs a large number of hashing by modifying a random component of the block content until,

by chance, someone finds a “valid” hash that is smaller than the threshold. This is called proof of work (PoW) and serves the purpose to determine majority consensus. Indeed, in an anonymous distributed system, participants can arbitrarily generate new identities so consensus cannot be accounted in terms of individuals. Rather, it must be accounted in terms of some participation cost demonstrating the commitment of computational power. In the words of Satoshi Nakamoto, “one CPU one vote” (Nakamoto, 2019). Bitcoin mining hardware has moved from CPU first to GPU (McNally et al., 2018) and later FPGA and ASIC but the principle behind the proof of work remains the same.

The network incentivizes users to participate in the block validation process by assigning newly mined Bitcoins to the first user who randomly finds a hash with a value smaller than the threshold. Presently, after the latest Bitcoin halving, this remuneration is 6.25 Bitcoins or around USD 60,000 at the current exchange rate (see Table 1). For this reason, the hashing process is called “mining” and miners often join to form large mining pools to have a more stable source of income (Gervais et al., 2014).

Sometimes forks occur in the blockchain when two blocks containing different transactions are attached to the same block. Eventually other blocks are mined and attached to them, forming two branching chains after the fork. In this case, the longer chain, the one with more cumulative proof of work or hash computations, would be considered as the main chain upon which future blocks are built on. Normally a block is considered finally valid after six blocks are attached to its chain, which takes ~1 h.

The Bitcoin proof of work is very costly economically (Thum, 2018) and environmentally (Stoll et al., 2019). Technological improvements over the years have made hashing a very efficient operation, consuming at little as 0.03 joules per billion hashes (with specifically-designed Application-Specific Integrated Circuit, ASIC, machines. See Table 2). This has reduced energy cost per hash by about thirty thousand times during the last 10 years. However, the miners in the Bitcoin network are presently (May 2020) computing nearly  $10^{25}$  hashes per day, up over 10 orders of magnitude from the 2010 levels. We estimate in this paper that this hashing activity currently corresponds to an energy cost of around 1 million USD per day and around a billion USD over the past year. In turn, this corresponds a per transaction costs as high as 13 USD in January 2020. This cost is not borne by either the sender nor the receiver in a transaction but rather by the miners. While a billion a year burned in hashing is definitely a large amount of

money that could be seen as a waste of resources, the Bitcoin proof of work is a necessary process for such an anonymous permission-less network to function. It is indeed required to validate transactions and obtain community consensus to secure the system from attacks.

One question arises: is this cost fair or could it be lowered? In Aste (2016) made the argument that, at equilibrium, the cost of Bitcoin proof of work should be such to make a double spending attack too expensive to be profitably carried out. From this principle, it is relatively straightforward to estimate the fair cost of the proof of work under an ideal equilibrium assumption. Let us consider an attacker that owns some amount of Bitcoin and wants to artificially multiply it by spending the same Bitcoin with several different users. This is known as a double spend attack. The attacker will try to double spend the largest amount of Bitcoin possible, but this is limited to the amount normally exchanged within a block (which, we estimate in this paper, is currently around \$10 million). Indeed, a transaction involving a substantially larger sum than the usual will capture unwanted attention from the network. Of course, the duplication can be repeated several times both in parallel or serially but, as we shall see shortly, this does not affect the outcomes of the present argument. To be successful the attacker must make sure that both the duplicated transactions are validated and this requires the generation of a fork with two blocks containing the double spent transaction attached to the previous block. If the attacker has sufficient computing power, she can generate two valid hashes to seal the two blocks giving the false impression that both transactions have been verified and validated. However, for a final settlement of the transaction, it is presently considered that one should wait six new blocks to be attached to the chain to make the transaction statistically unlikely to be reverted. The attacker should therefore use her computing power to generate six valid

**TABLE 1** | Bitcoin reward per block mined.

Start date	Bitcoin reward
3 Jan 2009	50.00
28 Nov 2012	25.00
9 Jul 2016	12.50
11 May 2020	6.25

**TABLE 2** | Mining hardware with optimal energy efficiency and their dates of release.

Type	Hardware name	Date	J/Th
CPU	ARM Cortex A9	3 Oct 2007	877,193
GPU	ATI 5870M	23 Sep 2009	264,550
FPGA	X6500 FPGA Miner	29 Aug 2011	43,000
ASIC	Canaan AvalonMiner Batch 1	1 Jan 2013	9,351
ASIC	KnCMiner Jupiter	5 Oct 2013	1,484
ASIC	Antminer U1	1 Dec 2013	1,250
ASIC	Bitfury BF864C55	3 Mar 2014	500
ASIC	RockerBox	22 Jul 2014	316
ASIC	ASICMiner BE300	16 Sep 2014	187
ASIC	BM1385	19 Aug 2015	181
ASIC	PickAxe	23 Sep 2015	140
ASIC	Antminer S9-11.5	1 Jun 2016	98
ASIC	Antminer R4	1 Feb 2017	97
ASIC	Ebang Ebit 10	15 Feb 2018	92
ASIC	8 Nano Compact	1 May 2018	51
ASIC	Antminer S17	9 Apr 2019	36
ASIC	Antminer S19 Pro	23 Mar 2020	30

hashes before the double spent transaction might be considered settled. Note that only one of the two forks (the shortest) must be artificially validated by the attacker since the other will be considered valid by the system and can be let to propagate by the other miners. Of course, it is quite unrealistic to assume that nobody notices the propagating fork for such a long time, but let's keep this as a working hypothesis. The artificial propagation of the fork has a cost that is the cost of the proof of work per block times six. The attacker will make profits if this cost is inferior to the gain made from duplicated spending. In the previous unpublished note by Aste (2016) the following formula is reported:

$$\begin{aligned} & \text{Equilibrium fair cost of proof of work per block} \\ &= \frac{\text{Duplicated fraction of the value of a block}}{\text{Number of blocks required for settlement}}. \end{aligned} \quad (1)$$

We can re-write this formula to formally express the cost of proof of work per day,  $C_t$ , as

$$C_t = \frac{pV_t}{N} \quad (2)$$

where:

$p$  is the duplicated proportion of block transaction volume;

$V_t$  is the average transaction volume on day  $t$ ;

$N$  is the number of blocks required for settlement.

In Equation (2)  $N$  is roughly equal to 6 and the current average volume of transaction is about  $V_t \sim 1$  billion USD a day but it was only a few thousands dollars a day in 2010. The value of  $p$  must be considerably smaller than one because an attacker will be spotted immediately by the community if she tries to fork with a large double-spent value with operations that involve a significant portion of the entire network activity. We must note that this formula is an upper bound for the cost of the proof of work. It greatly underestimates the costs of an attack and largely overestimates the attacker's gains. It indeed considers a system that has no other protections or security system than the proof of work. Further, it does not consider that after a successful attack, the Bitcoin value is likely to plunge making it therefore unlikely for the attacker to spend her gain at current market value. Finally, we should take into account that the attacker must have control over more than 50% of the hashing power. This requires either huge investments in mining equipment (not taken into account in the formula) or other methods to control the mining farms, such as through a cyber or a conventional physical attack, which will also cost considerable amount of money. Therefore, we expect the parameter  $p$  to be of the order of 1% or less.

Independently on the estimate of a realistic value for the parameter  $p$ , the principle that the cost of the proof of work must be a sizable fraction of the value transferred by the network to avoid double spending attacks should rest valid (Aste, 2016; Aste et al., 2017). Specifically, according to this principle, we expect that, for a given system, the ratio between the cost of the proof of work and the value transferred by the network should oscillate around some constant value which reflects the fair balance between the possible gains in an attack and the cost to perform it. In this paper, we test if this is indeed the case

for the Bitcoin proof of work. For this purpose we are looking across the entire period of existence of Bitcoin, estimating the mining costs and comparing them with the value transferred through the network. This is an amazing period during which the value transferred through the Bitcoin network has increased several million times and the hashing activity has increased by 10 orders of magnitude. Let us note that ten orders of magnitude is an immense change. To put it into perspective this is the ratio between the diameter of the sun and the diameter of a one-cent coin. These are formidable changes to a scale never observed in financial systems or in human activity in general. We show in this paper that, despite these underlying formidable changes in the Bitcoin mining and trading activities, the ratio between the estimated mining cost and the transaction volume rests oscillating within a relatively narrow band supporting therefore the argument about the fair cost of the proof of work by Aste (2016).

## 2. METHODOLOGY

### 2.1. Estimation of the Lower Bound for the Cost of Bitcoin Mining

The cost of Bitcoin mining is composed of three key elements:

1. The energy cost of mining
2. The overheads for the maintenance of the mining farm, such as infrastructure costs and cooling facilities
3. The cost of purchasing and renewing the mining hardware

For the purpose of this study, we focus only on the first element, the energy cost of running the Bitcoin mining hardware which is likely to be the key driver and is the only cost that can be estimated with some precision. The maintenance costs for running a Bitcoin mining farm varies widely depending on the location, design and scale of the facility and since such information are usually not disclosed to the public, it is infeasible to estimate it accurately. The sales price of mining hardware is publicly available but incorporating it into cost calculations is arduous because of the rapid rate of evolution in the industry and the information opacity regarding the market share of each hardware and the rate at which obsolete mining hardware are replaced. Newer mining hardware may achieve faster hash rates and higher energy efficiency but the renewing costs makes it unlikely that all Bitcoin miners immediately replace all their existing mining hardware with the latest versions as they are released. Certainly a combination of both old and new mining hardware should coexist in the Bitcoin network as long as each machine continue to generate a profit. However, the market share of each hardware and its evolution over time is an unknown. With respect to the purpose of the present estimate of the lower bound of the mining cost, we must stress that the maintenance and the hardware costs must be anyway proportional to the energy consumption costs. By ignoring them we are underestimating the total mining cost by some factor but, beside this factor, the estimation of the overall behavior of the mining cost should not be significantly affected.

## 2.2. Data

Historic data on Bitcoin prices, the average hash rate, and the number of daily blocks per day can be found on <https://charts.bitcoin.com/btc> and the estimated total value of all transactions on the Bitcoin network on <https://www.blockchain.com/charts/>. Hash efficiency and other information regarding Bitcoin mining hardware were aggregated from manufacturer data and previous studies (Küfeoğlu and Özkuran, 2019) and independently verified.

Most prior works have priced energy usage according to global average electricity prices (see for instance Vranken, 2017; Derks et al., 2018; Küfeoğlu and Özkuran, 2019). In this paper, we introduce a different approach, by converting the energy consumed during Bitcoin mining into barrels of oil equivalent and priced according to the Brent Crude spot price. Historical Brent Crude oil spot prices were collected from the EIA<sup>1</sup> with the conversion rate between joules and barrels of oil equivalent set at 1 barrel = 5.54543 gigajoules based on the figures released by the BEIS<sup>2</sup>. Our rationale is that the Brent Crude oil price is a publicly available daily value standardized around the world whereas electricity prices varies widely across different countries and suppliers. Note that there is a premium that electricity producers and distributors charge on the electricity price with respect to the oil cost and there can be also taxes. These extra charges depends on countries and situations but they will add a certain percentage to our estimate of the mining cost based on oil prices.

As another point of comparison, regional electricity prices were also used as a proxy for the energy cost. The average global electricity price used for mining was calculated based on the geographic distribution of hash rate on the Bitcoin network and the local industrial electricity price. Based on the figures released by the CCAF at [https://cbeci.org/mining\\_map](https://cbeci.org/mining_map), China, USA and Russia are responsible for over 80% of global hash rates. An overwhelming proportion of Bitcoins are mined in China so the data there is further stratified based on provinces. They are shown in **Table 3**. The three nations also publish government statistics regarding industrial electricity prices on a regular basis (China: NEA, USA: EIA, Russia: Petroelectrosbyt) which allowed for the annual weighted average electricity price for Bitcoin mining,  $E_t$ , to be calculated as

$$E_y = \sum_i w_i p_i \tag{3}$$

where:

$i$  is the set of regions in **Table 3**;

$w_i$  is the share of global hash rate accounted for by region  $i$ ;

$p_i$  is the industrial electricity price in region  $i$ , converted to USD/kWh based on the average exchange rate.

A disproportionately large percentage of mining activity within China was based in provinces with lower than average electricity prices so where provincial data were not available, a 0.738 multiplier based on empirical data from 2013 to 2018

<sup>1</sup><https://www.eia.gov/dnav/pet/hist/rbrteD.htm>

<sup>2</sup><https://assets.publishing.service.gov.uk/government/uploads/system/uploads/>

**TABLE 3 |** Geographic distribution of the share of hash rate on the Bitcoin network, 2019–2020.

Nation/Provinces	% of global hash activity
China	71.70
- Xinjian	30.13
- Sichuan	18.58
- Inner Mongolia	7.71
- Yunnan	7.07
- Gansu	2.02
- Beijing	1.37
- Zhejiang	1.06
- Other provinces	3.76
Russia	6.08
USA	5.29

was applied on national Chinese electricity prices to calculate  $E_{China}$ . Regional share of hash rate and electricity prices were not available for USA or Russia so similar adjustments weren't possible. Another limitation of electricity prices is that a growing proportion of Bitcoin mining uses low-cost stranded renewables (Andoni et al., 2019), such as the use of associated gas that would otherwise be flared (Loris, 2019) which could further lower the energy cost of Bitcoin mining below the national averages. Due to these other factors and the lack of historic data on electricity prices in several other countries around the world, the majority of this paper will focus on energy pricing using the Brent Crude oil index. A comparison of ratio between the cost of mining and Bitcoin transaction volume is presented in **Figure 6** to show the standardized oil prices as a measure of energy cost yield similar results to using regional electricity prices.

## 2.3. Estimation of the Energy Costs of Bitcoin Mining

A mining hardware has an energy consumption that can be measured in joules per terahash (J/Th), and has a hashing speed that can be measured in terahashes per second (Th/s). For the purpose of estimating a lower bound to the energy costs of Bitcoin mining, we considered at any point in time that the entire network is adopting the most energy efficient machine available at that time. In situations where a mining hardware has different power setting options in which the user may choose to increase or decrease the hashing speed of the machine along with energy consumption, the most efficient power setting is used for calculation.

The lower bound of the energy costs of Bitcoin mining is estimated from total number of hashes times the energy cost of hashing by the most energy efficient Bitcoin mining hardware available on the market at any give time, divided by the conversion factor between energy and barrel of oil and multiplied by the cost of the oil. Specifically, the lower bound for daily mining cost,  $C_t$ , is:

$$C_t = \frac{e_t H_t}{b} P_t \tag{4}$$

where:

$e_t$  is the energy efficiency of the most efficient mining hardware available on day  $t$  in (J/Th);

$H_t$  is the daily number of hashing operations in (Th) on day  $t$ ;

$b$  is the joule of energy equivalent per barrels of oil  $\approx 5.55 \times 10^9$  (J/barrel);

$P_t$  is the Brent crude oil spot price (USD/barrel) on day  $t$ .

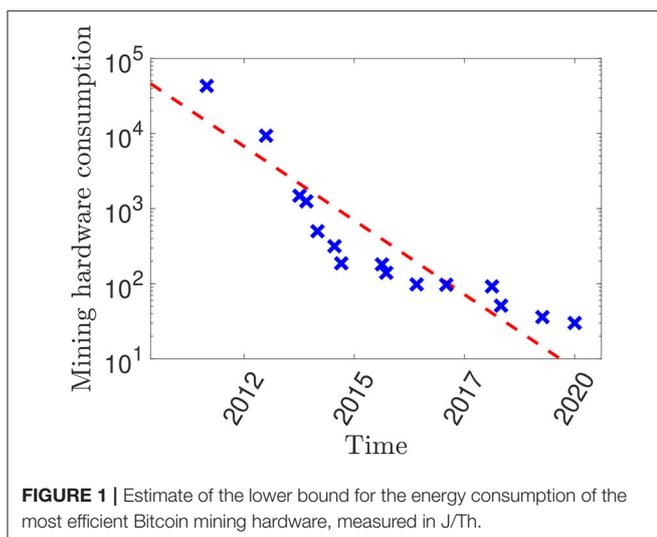
### 3. RESULTS

#### 3.1. Hardware Efficiency Variations

Table 2 reports a list of the Bitcoin mining hardware which consumed the least energy per hash operations at the time of their release to the market. The improvement in energy efficiency for Bitcoin mining over time is reported in Figure 1 where each symbol represents the most energy efficiency hardware at the respective time and the red dotted line displays a best-fit with an exponential curve: Energy Consumption  $\sim c \exp(-\lambda t)$ . The best fit parameter is  $\lambda = 0.0025$ , which means that hardware efficiency has been doubling every 10 months in average. In a previous work a power-law model was proposed by Kristoufek (2020). However, the exponential model is more consistent with what is commonly expected for the rate of technology growth, according to the Moore’s Law (Moore, 1998).

#### 3.2. Hash Computations Variations

Figure 2 displays the total number of hashing operations per day. We note that the number of daily hashes have increased from  $10^{15}$  to  $10^{25}$  in the period between September 2010 to May 2020 when this paper was written. Daily hashes have been growing at exponential rates (linear trends in semi-log scale), which is in agreement with previous observations (O’Dwyer and Malone, 2014). However, we can see from the figure that there are four, very distinct, periods with different grow rates. Specifically: (i) mid 2010 to mid 2011; (ii) mid 2011 to early 2013; (iii) early 2013 to early 2015; (iv) early 2015 to early 2020. The estimated best-fit doubling times in these periods are respectively: (1) 33 days; (ii) 261 days; (iii) 38 days; (iv) 198 days.

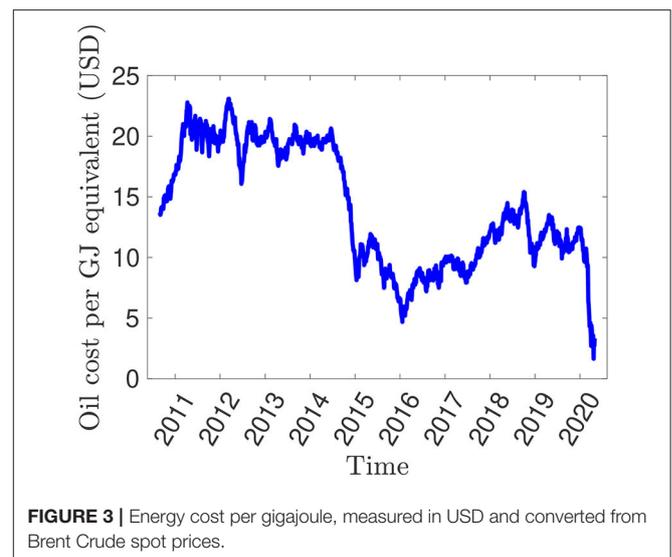
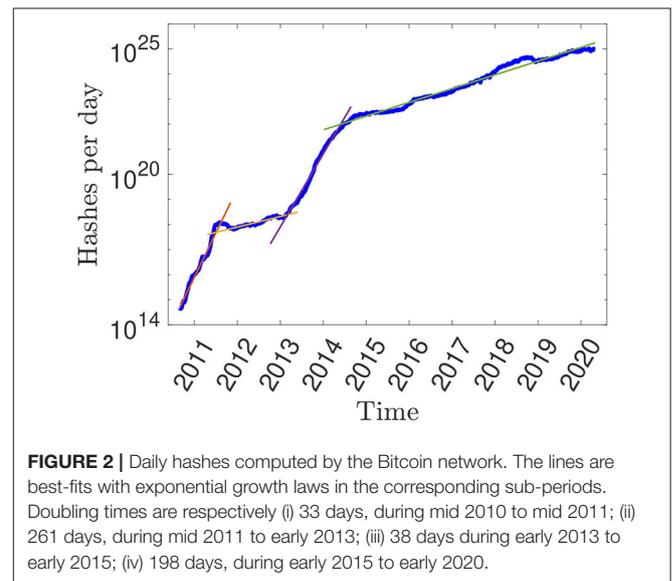


#### 3.3. Energy Price Variations

Figure 3 shows the variations of the energy price per gigajoule in the period 2010–2020 computed from the Brent Crude spot prices. One can notice that the cost of one gigajoule of energy has two distinct levels—around 20 USD from 2011 to mid 2014 and around 10 USD from late 2014 to early 2020. Oil prices has since collapsed under the coronavirus pandemic, dropping to below 3 USD per gigajoule of energy. However, while large, the rate of change in energy price is several orders of magnitude smaller than the rate of change in the number of hashes.

#### 3.4. Lower Bound Mining Cost Estimate

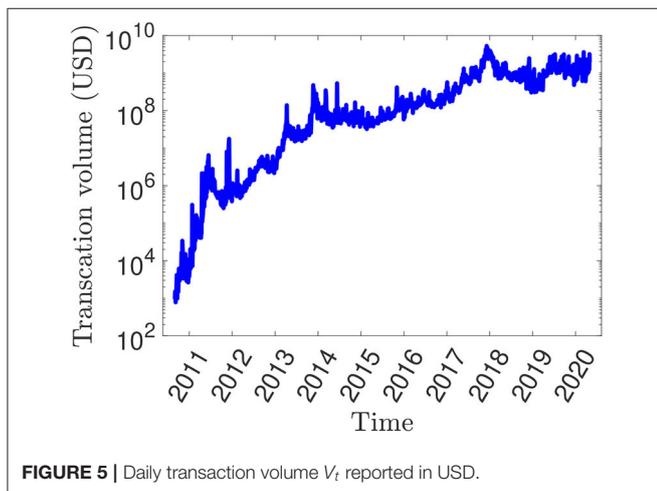
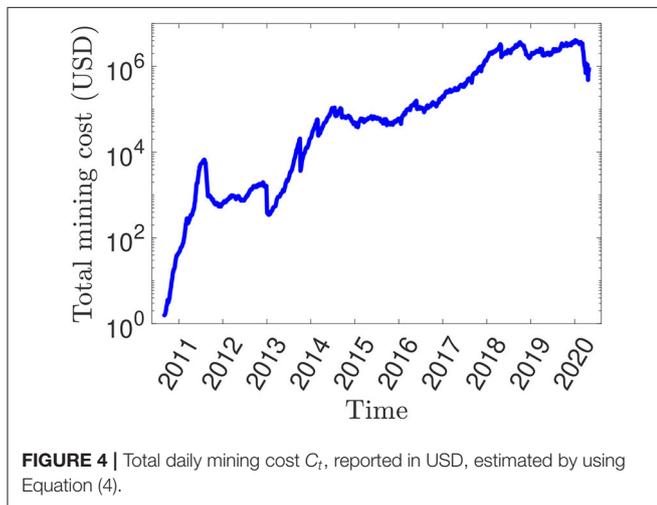
The lower bound of the total energy costs of Bitcoin mining is estimated as the minimum energy cost of each hash multiplied by the total number of hashes computed over a given period



of time (a day in our case). **Figure 4** reports the total mining daily cost in USD estimated by using Equation (4), it varies from around 3 USD a day in 2010 to over 4 million USD a day in early 2020. Note that this is the lower bound estimate and the actual cost is presumably much larger. The growth in mining costs is affected by both the changes in energy cost (see **Figure 3**) and by the increase in the hashing rate in the Bitcoin network (see **Figure 2**). We note that the variations in energy cost oscillates in a much narrow band with respect to the changes in the daily number of hashes and therefore, the minimum Bitcoin mining costs (**Figure 4**) mostly mirrors the growth in the total number of hashes.

### 3.5. Transaction Volume Variations

During the last 10 years the Bitcoin network activity has also increased with increasingly larger amount of money transferred daily through the network. **Figure 5** reports the total transferred value per day in the Bitcoin network specified in USD. One can see that the total daily volume of transactions has grown from



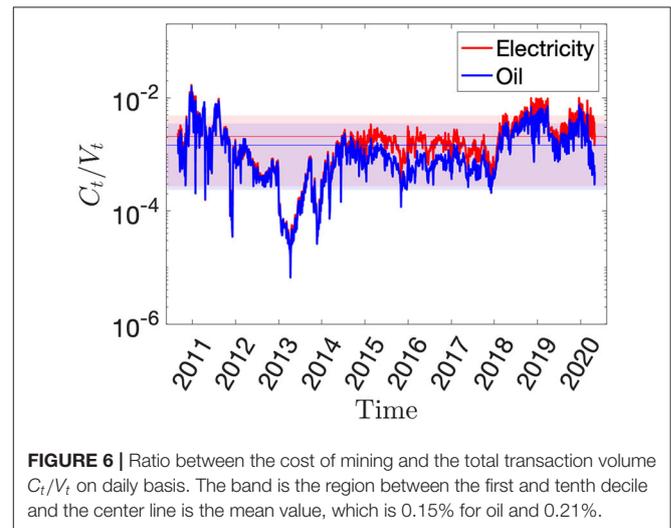
about one thousand USD in 2010 to nearly one billion USD in 2020 for an increase by six orders of magnitude.

### 3.6. Ratio Between Mining Cost and Transaction Volume

**Figure 6** reports the ratio between the daily mining cost  $C_t$  and daily transaction volume  $V_t$ . We observe that the ratio  $C_t/V_t$  does not have any increasing or decreasing trend but rather is oscillating within a certain band over most of the period from 2010 to 2020. The largest variations occurred in the first few years then, after 2014, the ratio value has stabilized into a plateau with then a jump to a higher plateau at the end of 2017 presumably due to the large decrease in Bitcoin price from over 19,000 USD in December 2017 to just a little over 3,000 USD in December 2018. Despite the change in this relation between mining costs and transaction volume in 2017–18 and the change in Bitcoin prices in the same period, we note that in general this ratio is not correlated with the price of Bitcoin. There is actually a small negative correlation between the two for the daily variations. Over the entire period, the mean value of  $C_t/V_t$  is 0.15% with the first decile being 0.02% and tenth decile being 0.4%. Using regional electricity prices to calculate the mining costs shows a similar pattern over time, though on a slightly higher level after 2014 with the mean ratio being 0.21%. Note that this band of oscillation is within one order of magnitude whereas the underlying quantities  $C_t$  and  $V_t$  vary of six orders of magnitude during the same period. If we limit our analysis to the last period after the end of 2017, we obtain a mean ratio of 0.3% and D1, D10 deciles with values equal to 0.1 and 0.4%.

## 4. DISCUSSION AND CONCLUSIONS

The proof of work allows a network of anonymous and untrustful parties to operate together without central authority control. It is a powerful instrument to keep a distributed system secure from malicious attacks. However, it has a high cost. We estimate that



presently at least a billion USD per year is burned by the Bitcoin network for the proof of work. This amount corresponds to a one million times increase with respect to the costs in 2010. However, although large, this amount is  $<0.5\%$  of the transaction volume over the network during the same period.

Using data from 2009 to 2020, this paper quantifies the lower bound for the energy costs of Bitcoin mining and examines the relationship between this bound to the total value of transactions over time. We reveal that the ratio between mining cost and total transaction volume has not increased nor decreased over the last 10 years despite Bitcoin mining activity having increased by ten billion times during the same period. Such an overall constant ratio is consistent with an argument, introduced by Aste (2016), suggesting that such a ratio must be a sizable fraction of the transaction volume and it corresponds to the minimum fraction that an attacker must double spend to make a profit (the quantity  $p$  in Equation 2). Assuming the default block depth of  $N = 6$  in Equation (2), and using the last 3 years mean value for the fraction  $C_t/V_t$  at  $\sim 0.3\%$ , we obtain that Bitcoin proof of work protects from a double spend attack at least a fraction around  $p \sim 1.5\%$  of the global transaction volume. This result indicates that attacks that duplicate more than  $\sim 1.5\%$  of the transaction volume could be profitable for the attacker because the cost of energy spent for the attack will be lower than the gain from the attack. This being a lower bound estimate that realistically could be an order of magnitude larger if all extra costs, beside the oil equivalent cost of mining energy, are included.

We could therefore conclude that in the Bitcoin network the cost of proof of work is not at all too high. On the contrary it is actually too low to protect against double spending attacks. However, the proof of work is not the sole mechanism that provides protection of the Bitcoin network. The system also depends upon the high entry barriers in terms of mining hardware and facilities costs. Further, Bitcoin value is built upon community trust so once a majority attack has been detected, the Bitcoin value is likely to collapse together with the potential attacker gains. This means that to launch a majority attack on Bitcoin, the attacker would thus not only need to invest substantial amounts of energy resources to gain over 50% of

the hashing power, they would also have to accept that many of the hardware costs incurred are unlikely to be recovered due to the inability of specialized ASICs to be repurposed for uses other than cryptocurrency mining and that even if the attack was successful, the value of Bitcoin would collapse so rapidly that there would be little economic gain. Finally, an attack involving a large fraction of the Bitcoin volume would be most likely detected by the network before its completion.

Distributed systems and Blockchains can be secured through several other mechanisms that do not require computationally intensive proof of work. Indeed the proof of work is a mechanism introduced to produce qualified voters in a system of anonymous untrustful parties. Any mechanism that can verify identity of the voters' or that can in any other way avoid uncontrolled duplications of the voters can reduce or eliminate completely the cost and even the need of a proof of work. However, these other mechanisms must relax also some other properties, such as anonymity, openness, or equalitarian distributed verification.

## DATA AVAILABILITY STATEMENT

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

## AUTHOR CONTRIBUTIONS

TA proposed the research, supervised and contributed to the data collection, performed the data analytics, and co-drafted the paper. Y-DS collected, processed and analyzed the data, and co-drafted the paper. Both authors gave final approval for publication and agree to be held accountable for the content of the work.

## ACKNOWLEDGMENTS

TA acknowledges support from ESRC (ES/K002309/1), EPSRC (EP/P031730/1), and EC (H2020-ICT-2018-2 825215). This article has been released as a pre-print to arXiv as Song and Aste (2020).

## REFERENCES

- Akcora, C. G., Dey, A. K., Gel, Y. R., and Kantarcioglu, M. (2018). "Forecasting bitcoin price with graph chainlets," in *Pacific-Asia Conference on Knowledge Discovery and Data Mining* (Melbourne, VIC: Springer), 765–776. doi: 10.1007/978-3-319-93040-4\_60
- Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., et al. (2019). Blockchain technology in the energy sector: a systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* 100, 143–174. doi: 10.1016/j.rser.2018.10.014
- Aste, T. (2016). *The Fair Cost of Bitcoin Proof of Work*. SSRN. Available online at SSRN: <https://ssrn.com/abstract=2801048> (accessed March 3, 2020).
- Aste, T., Tasca, P., and Di Matteo, T. (2017). Blockchain technologies: the foreseeable impact on society and industry. *Computer* 50, 18–28. doi: 10.1109/MC.2017.3571064
- Blockchain.com (2020). *Market Capitalization*. Available online at: <https://www.blockchain.com/en/charts/market-cap?timespan=all> (accessed January 21, 2020).
- Chan, W. H., Le, M., and Wu, Y. W. (2019). Holding bitcoin longer: the dynamic hedging abilities of bitcoin. *Q. Rev. Econ. Finance* 71, 107–113. doi: 10.1016/j.qref.2018.07.004
- Derks, J., Gordijn, J., and Siegmans, A. (2018). From chaining blocks to breaking even: a study on the profitability of bitcoin mining from 2012 to 2016. *Electron. Markets* 28, 321–338. doi: 10.1007/s12525-018-0308-3
- Gervais, A., Karame, G. O., Capkun, V., and Capkun, S. (2014). Is bitcoin a decentralized currency? *IEEE Secur. Priv.* 12, 54–60. doi: 10.1109/MSP.2014.49
- Grobys, K., and Sapkota, N. (2019). Cryptocurrencies and momentum. *Econ. Lett.* 180, 6–10. doi: 10.1016/j.econlet.2019.03.028
- Kristoufek, L. (2020). Bitcoin and its mining on the equilibrium path. *Energy Econ.* 85:104588. doi: 10.1016/j.eneco.2019.104588
- Küfeoğlu, S., and Özkuran, M. (2019). Bitcoin mining: a global review of energy and power demand. *Energy Res. Soc. Sci.* 58:101273. doi: 10.1016/j.erss.2019.101273
- Loris, N. (2019). *Pursuing Policies to Drive Economic Growth and Reduce Emissions*. Background, No. 3444.

- McNally, S., Roche, J., and Caton, S. (2018). "Predicting the price of bitcoin using machine learning," in *2018 26th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)* (Cambridge, UK: IEEE), 339–343. doi: 10.1109/PDP2018.2018.00060
- Moore, G. E. (1998). Cramming more components onto integrated circuits. *Proc. IEEE* 86, 82–85. doi: 10.1109/JPROC.1998.658762
- Nakamoto, S. (2019). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Technical report, Manubot.
- O'Dwyer, K. J., and Malone, D. (2014). "Bitcoin mining and its energy footprint," in *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies* (Limerick), 280–285. doi: 10.1049/cp.2014.0699
- Sin, E., and Wang, L. (2017). "Bitcoin price prediction using ensembles of neural networks," in *2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)* (Guilin: IEEE), 666–671. doi: 10.1109/FSKD.2017.8393351
- Song, Y.-D., and Aste, T. (2020). The cost of Bitcoin mining has never really increased. *arXiv* 2004.04605. doi: 10.2139/ssrn.3574512
- Stoll, C., Klaaßen, L., and Gallersdörfer, U. (2019). The carbon footprint of bitcoin. *Joule* 3, 1647–1661. doi: 10.1016/j.joule.2019.05.012
- Thum, M. (2018). "The economic cost of bitcoin mining," in *CESifo Forum*, Vol. 19 (München: ifo Institut-Leibniz-Institut für Wirtschaftsforschung an der Universität München e.V.), 43–45.
- Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Curr. Opin. Environ. Sustain.* 28, 1–9. doi: 10.1016/j.cosust.2017.04.011

**Conflict of Interest:** The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

*Copyright © 2020 Song and Aste. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.*