From chaining blocks to breaking even: A study on the profitability of bitcoin mining from 2012 to 2016

This version: February 2018

Abstract

Bitcoin is a widely-spread payment instrument, but it is doubtful whether the proof-of-work (PoW) nature of the system is financially sustainable on the long term. To assess sustainability, we focus on the bitcoin miners as they play an important role in the proof-of-work consensus mechanism of bitcoin to create trust in the currency. Miners offer their services against a reward while recurring expenses. Our results show that bitcoin mining has become less profitable over time to the extent that profits seem to converge to zero. This is what economic theory predicts for a competitive market that has a single homogenous good. We analyze the actors involved in the bitcoin system as well as the value flows between these actors using the *e³value* methodology. The value flows are quantified using publicly available data about the bitcoin network. However, two important value flows for the miners, namely hardware investments and expenses for electricity power, are not available from public sources. Therefore, we contribute an approach to estimate the installed base of bitcoin hardware equipment over time. Using this estimate, we can calculate the expenses miner should have. At the end of our analysis period, the marginal profit of mining a bitcoin becomes negative, i.e., to a loss for the miners. This loss is caused by the consensus mechanism of the bitcoin protocol, which requires a substantial investment in hardware and significant recurring daily expenses for energy. Therefore, a sustainable crypto currency needs higher payments for miners or more energy efficient algorithms to achieve consensus in a network about the truth of the distributed ledger.

JEL-classifications O16, O39
Keywords: bitcoin, business model, financial sustainability, mining, POW

1 Introduction

Since bitcoin emerged in 2009, individuals and companies invested billions of dollars in the digital currency and the underlying blockchain technology. The bitcoin is an unregulated digital peer-to-peer currency with a finite supply of 21 million units that is not backed by debt obligations and governments (Grinberg, 2012) and does not need third parties such as banks (Courtois & Bahack, 2014). Although the bitcoin firstly is a payment instrument, it also serves as an incentive given to blockchain providers, referred to as 'miners', who provide the computing power needed for clearing transactions in the bitcoin network (Nakamoto, 2008). The bitcoin currency provides a certain degree of anonymity, has no issuance expenditure and charges none to low transaction fees (Nakamoto, 2008). The bitcoins can be obtained by purchasing them, generating them by acting as a miner, earning them in exchange for an activity of service, receiving them as a form of payment or receiving them as a donation/gift (Plassaras, 2013; European Central Bank, 2015). Current uses for bitcoin are payments to (online) merchants, sending remittances abroad and speculation (Goldman Sachs, 2014; Bouoiyour & Selmi, 2015).

The European Central Bank (ECB) considers bitcoin to be a digital representation of value, not issued by a central bank. It can serve as a substitute to banknotes, coins, demand deposits and e-money. Currently, most national banks in the European Monetary Union follow the example of the ECB by issuing a warning about the risks of bitcoin, but there is no framework for regulation (European Central Bank, 2015).

This lack of regulation and backing of the bitcoin has led to a freely developing economic system in which millions of dollars' worth of fiat currencies are spent to buy and trade bitcoins. On top of this, investment firms made large investments in bitcoin-related companies (Edgar Fernandes, 2014; Davies, 2015). Many parties profited from the increased value of the bitcoin,

but some went bankrupt (Ember, 2015) or had to suspend services when its value dropped (Ember, 2015; Higgins, 2015).

The bitcoin network exposes a number of issues: amongst others the scalability, speed and consensus system are known problems for bitcoin (see Decker and Wattenhofer, 2015; Barber et al., 2012; Forte et al., 2016). In this paper however, we address another important problem of the bitcoin work and that is its long term economic sustainability. The promise of the bitcoin network is to provide a transaction processing engine and payment instrument; if this really happens, such an instrument should be economically sustainable in order to replace the traditional payment system of banks.

To answer the question of long-term sustainability, we quantify the most important revenue streams in the bitcoin network. We utilize network theory on networked value constellations, and more specifically the *e*^{3}*value* methodology (Gordijn & Akkermans, 2003) to understand the ecosystem of enterprises and end-users. The *e*^{3}*value* method requires that each actor in an ecosystem is capable of generating a net cash flow on the long term. If one or more actors fail to do so, the network collapses and is unsustainable. The methodology supposes that participants in a system are rationally behaving actors to do a best-effort to generate cash flow. The *e*^{3}*value* method is backed by theory on networked value constellations (e.g. Tapscott, Ticoll & Lowy (2000), Normann & Ramirez (1994), and also Porter, (1985)), axiology (e.g. Holbrook (1999)), and traditional well-known investment theory such as discounted net present value calculations, break even analysis and payback time.

Our analysis of the bitcoin network will reveal a number of actors, for which we assume that most of them *are* actually capable of generating a net cash flow (for example the providers of hardware and electricity supply companies). As a result of this assumption, the evaluation of

the sustainability of the bitcoin network focuses on the financial risks of the *miners* that keep the bitcoin network secure and trustworthy.

From 2012 to 2016, miners of the bitcoin network created over $2bln worth of bitcoin in exchange for the security and transaction clearances they offered to the users. To earn these revenues, large investments in specialized hardware were required, as well as operational expenses in electricity power. In short, the value of the mined bitcoins should outweigh the expenses. There is a vast body of public data available about the bitcoin (e.g. the number of transactions per day and the exchange rate) but in order to calculate the expenses of the miner we need to know the installed base of mining hardware of time, as this installed base results in investments and energy expenses. Unfortunately, information about the installed base is not available. Therefore, in this paper we develop an estimate of this installed base assuming that miners do rational decision making. This estimate of the installed base over time, and how to do that estimate is the main contribution of this paper.

The rest of the paper proceeds as follows: In Section 2 we review the bitcoin system to capture the ecosystem of the bitcoin. Section 3 presents the overall research approach. We use a model-based approach (*e*^{3}*value*) to understand the bitcoin ecosystem (Section 4). In Section 5, we quantify the revenues and expenses of miners for a period of five years. As we will discuss further in Section 6, the marginal revenues of miners approach the marginal expenses (mainly related to electricity costs). As a result, bitcoin mining moves from a highly profitable business to an undertaking that is, on average, barely returning the investment in hardware.

2 The bitcoin system

Payment innovation

Bitcoin is fundamentally different from trust-based electronic payment systems where financial intermediaries (e.g. banks) process payments, mediate in disputes and are able to reverse payments. With these trust-based systems, the intermediary checks if the sender of the payment can afford the payment, preventing them from spending the same amount of money twice (also called the double spending problem). The bitcoin network also offers payment services, but does so in a decentralized way, meaning that trust-based parties, such as banks, are not needed. Opposite to trust-based systems, bitcoin transactions are non-reversible and the network offers no mediation in disputes.

Banks have pioneered in the adoption of electronic markets for internal processes, but have been slow to do so in the field of consumer interaction (Alt & Puschmann, 2012). Bitcoin is a disruptive innovation as its goal is to entirely remove the middlemen namely the banks. Bitcoin does not require intermediaries to provide secure storage of funds. A bitcoin owner can store bitcoins on many kinds of devices by installing a software program called a bitcoin wallet. This has the disadvantage of placing the responsibility for safeguarding bitcoins on the owner, nor is any interest earned on the deposits.

Owners also often store their bitcoins on centralized exchanges in order for the exchange to safeguard the funds or to speculate on value changes. Storing bitcoins at centralized exchanges, poses the funds at considerable risk as a number of exchanges defaulted due to cyber-attacks, insolvency or outright fraud (Moore & Cristin, 2013).

The bitcoin system has a built-in mechanism that reduces the amount of newly created coins per block, to prevent inflation (Courtois & Bahack, 2014). By the beginning of 2017, about 16 of the total 21 million bitcoins were mined. Figure 2 shows the (projected) number of bitcoins that will go in circulation during the first ten years of the bitcoin network.

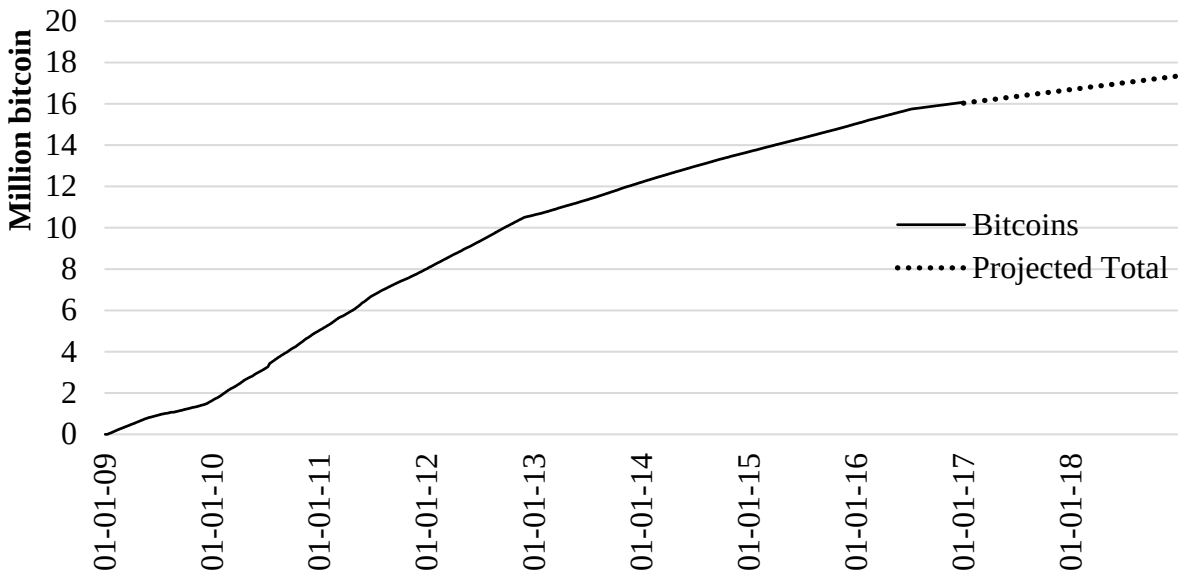

Figure 2 – bitcoins in circulation

Source: https://en.bitcoin.it/wiki/Controlled_supply

At the heart of bitcoin lies the blockchain technology that acts as a distributed, shared transaction ledger that records all transfers of bitcoins. Each block is like a new page of a ledger containing the most recent transactions. The network consists of nodes where the majority reaches a consensus on the transaction history and on which transactions are valid (Kroll, Davey and Felten, 2013).

Solution to the double spending problem

With fiat currencies, the double spending problem is solved as a third party like a bank can clear transactions or it can take the shape of physical cash. The bitcoin, however, is a neither a physical token nor a database record of a trusted bank representing the money. Instead, the bitcoin network consists of parties who cannot be trusted upon beforehand. Therefore, in principle, it would be simple to duplicate coins by some party, e.g., by paying twice with the same coin in two separate transactions. Without a trusted bank preventing users from spending the same money twice, another solution must be found. Blockchain technology, the basis of

bitcoin, employs a consensus mechanism that guarantees a majority of the participants in the network agree on the validity of transactions.

There are several ways to implement a consensus mechanism, and for bitcoin the chosen mechanism for validation of the bitcoin transactions occurs by an activity called ‘proof-of-work’, which is executed by miners (Courtois & Bahack, 2014; Courtois, Grajek, & Naik, 2013). Proof-of-work is a computationally hard problem (a cryptographic puzzle) solved by a significant amount of distributed computing power directly relating to the signing, and therefore approving, of a transaction block, including all earlier approved blocks (hence the name blockchain). Miners are incentivized to do the proof-of-work with their computers with a reward in the form of newly created bitcoins and possibly transaction fees. When a miner solves the cryptographic puzzle, it broadcasts the solution to other miners. Other miners easily verify this solution as the reverse computation is simple. If honest miners control more computer power than dishonest miners (Nakamoto, 2008), the bitcoin system as a whole is trustworthy. It is not possible for a minority of miners to manipulate transactions, as the network as a whole will not accept payments that were not issued by the owner of the bitcoins.

Next to proof-of-work miners, the bitcoin network is also supported by full nodes that do not receive a reward. These full nodes offer the user increased privacy and security that lightweight clients do not offer (Gervais et al. 2014).

Vulnerabilities

Many authors have analyzed the possibilities to attack the bitcoin network. Barber, Boyen, Shi, and Uzun (2012) mention several types of attacks like attempts at history-revision and the theft of bitcoins. Moore and Christin (2013) analyze attacks on bitcoin exchanges. A network-takeover attack scenario, which boils down to taking over the mining function by controlling over 50% of the mining power is a possibility (Davey & Felten, 2013). As the bitcoin reward

lowers over time, the transaction fees should reimburse the miners for securing the network, but over the last couple of years, these fees have been dropping (Möser & Böhme, 2015).

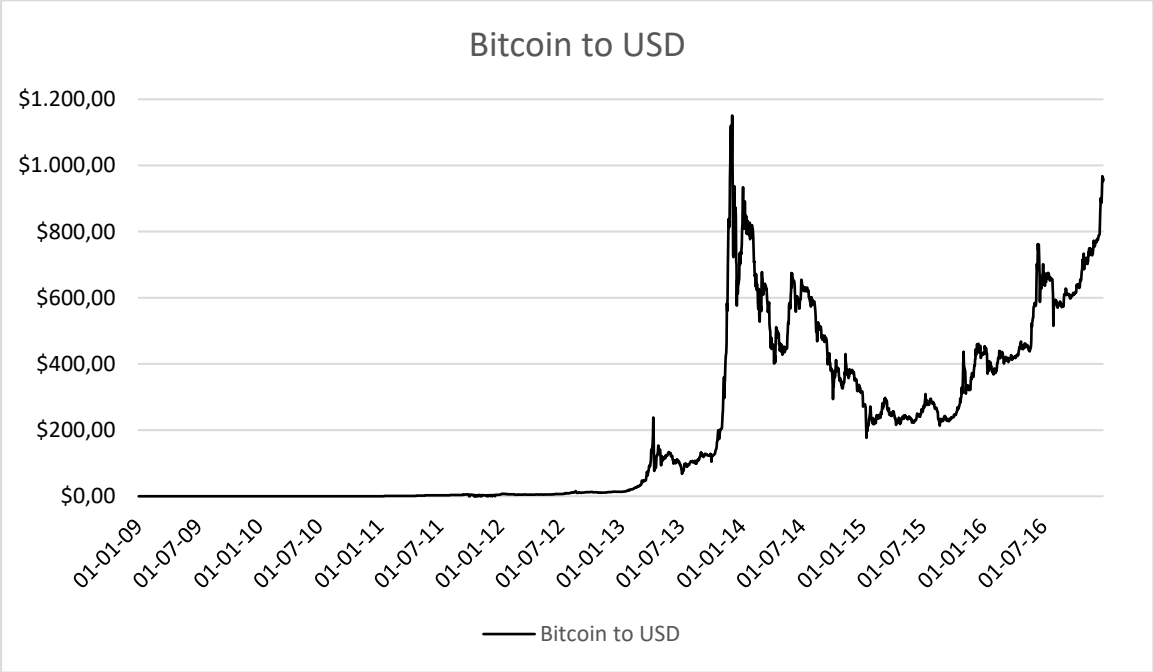

Figure 3 – Bitcoin value over time from 2009 to 2016 (in US-Dollars)

Source: https://blockchain.info/charts/market-price

As a unit of account, bitcoin is quite unstable. Figure 3 shows that during the first years of trading, the bitcoin was not widely traded putting its value close to zero. Trading took off in 2011, when one bitcoin was worth about $0.05. Early 2013, bitcoin peaked above $200, only to drop back in value later on again. During the final months of 2013, the value increased to over $1100 and dropped in the following months. During the early months of 2015, the value of bitcoin has been relatively stable between $200 and $300 and after rising since the end of 2015, the value rose above $900 again. The overall volatility of the bitcoin price makes it an unreliable unit of account.

Mining

Since bitcoin's inception, mining has changed from a small amateur activity to a multi-million-dollar business. By 2013, there were four generations of mining hardware in which energy efficiency increased by a factor of almost 10,000 (Courtois, Grajek & Naik, 2013). Due to the rapid decrease of hardware costs and the increase in energy efficiency, mining hardware quickly becomes outdated as newcomers, equipped with the newest hardware, are able to mine bitcoins at lower costs, increasing the network hash rate and lowering the return per gigahash per second (GH/s). GH/s is the performance rate for hardware, measuring the speed of solving the cryptographic puzzles that come with the bitcoin technology. The rapid progress in bitcoin mining technology makes bitcoin mining a risky venture.

Value is created every time a new block is mined and one of the miners is rewarded with new bitcoins and transaction fees. The reward is hard-wired into the blockchain software to incentivize miners to continually provide computing power to the network. As the miners keep the blockchain going, the bitcoin owners have the possibility to send transactions across it. For a transaction to be rapidly added into the blockchain, the owners can offer a transaction fee, as miners can choose to ignore transactions that do not offer a fee. In addition, the miners often use pools, where their mining effort is combined with that of others. In pools, when one miner finds the block, the rewards will be spread among all users of the pool according to their share in hashing power. This way, the miner will get a partial reward more quickly than when the miner would have mined on his own. In return, the owners of the pools often ask for a fee. The pools do not handle the mining of the block itself, but provide a block reward sharing service, so they are a service that concerns only the miners and not the bitcoin owners.

Miners have to invest in hardware and pay for electricity to keep the hardware running. In order to make a profit and pay some of the bills in fiat money, miners can sell a share of their mined

bitcoins via centralized online exchange websites. The miners need a bank account to receive the fiat currencies.

Our method of computing bitcoin investments and profits uses computations similar to those of bitcoin profitability calculators. Such calculators compute payback times and profits for given investments in hardware and energy prices. These calculators use a predicted decrease in profit that is of linear or exponential nature. We use historical hash rates and the available hardware at different points in time to reverse-engineer what has happened in the mining industry. This research is the first to provide an estimation of bitcoin mining net cash flows for the years 2012 to 2016. This provides insight into the actual profits on a daily basis and the sustainability of bitcoin mining.

3 Research approach

The key question to answer is:

RQ1: Is the bitcoin is a financially sustainable, long-term peer-to-peer paying service?

The bitcoin is considered to be financially sustainable if the participating actors are able to generate a net positive cash flow on the long term. During the research period there was no publicly available information about the expenses of bitcoin mining operations, and thus, no insight into the net cash flows.

To address the profitability of the participants in the network, we first have to understand the actors involved in the bitcoin ecosystem, as well as the revenue streams between these actors. To do so, we develop a networked business model, using the *e*^{3}*value* method, (Gordijn & Akkermans, 2003), which describes the total bitcoin system in an adequate way. The purpose of using the *e*^{3}*value* method is twofold. First, it results in a map of the actors involved as well as the objects of economic value in the exchange, called value objects. In many cases, these

objects reflect money but they can also be goods or services. Second, it allows for quantification of the value streams (specifically the monetary ones) and gives a long-term view of cash flows.

Construction of the *e³value* model

To construct the *e³value* model of the bitcoin ecosystem, we use a number of sources. Apart from our own knowledge about the bitcoin, we consult the literature, analyze publicly available information of the bitcoin, and finally perform ten interviews to validate the constructed models. The literature and public available data led to the creation of the *e³value* model that was validated in ten interviews.

Interviews

In 2014, a broad spectrum of stakeholders from the financial industry was interviewed:

1. Co-founder of bitcoin payment provider
2. Marketing manager at Dutch bitcoin exchange
3. Founder of bitcoin consultancy firm
4. Retired bitcoin miner
5. Member of Dutch Parliament
6. Policy Advisor Payment systems at De Nederlandsche Bank (Dutch Central Bank)
7. Bank examiner at De Nederlandsche Bank (Dutch Central Bank)
8. Project leader quality control financial products at AFM (Dutch financial authority)
9. Structured Finance Banker at ING Bank
10. Manager Pricing & Business Intelligence at ING Bank

During the interviews the following subjects were discussed:

1. **Details:** The job and organization of the interviewee.
2. **Personal POV:** The personal viewpoint on bitcoin.

3. **Organizational POV:** The viewpoint of the organization on bitcoin.
4. **E3 value model:** Discussion of the e3 value model.

The backgrounds of the interviewees can be divided into three groups: 1. Blockchain experts (1-4), 2. government officials (5-8) and 3. bankers (9 & 10).

Furthermore, to understand the bitcoin ecosystem, we develop an *e³value* business model describing the most important value streams in the bitcoin network based on the body of literature about the bitcoin available. The *e³value* model describes the actors (enterprises and individuals) involved and the things (called value objects) they exchange with each other (Gordijn & Akkermans, 2003). It is also possible to describe a group of actors who assign economic value in the same way; this construct is called the market segment. Furthermore, a key notion in *e³value* is the idea of economic reciprocity: actors exchange only something of economic value if they get something in return of higher value. If they do so, this will result in a net positive cash flow and therefore sustainability.

The *e³value* business model will be discussed with the interviewees and changed according to their feedback.

4 Value creation in the bitcoin ecosystem

To understand the bitcoin ecosystem, we develop an *e³value* business model describing the most important value streams in the bitcoin network. The *e³value* model describes the actors (enterprises and individuals) involved and the things (called value objects) they exchange with each other (Gordijn & Akkermans, 2003). It is also possible to describe a group of actors who assign economic value in the same way; this construct is called the market segment. Furthermore, a key notion in *e³value* is the idea of economic reciprocity: actors exchange only

something of economic value if they get something in return of higher value. If they do so, this will result in a net positive cash flow and therefore sustainability.

Figure 4 shows the actors and market segments that are relevant for the value creation in the bitcoin network. An interesting feature of the bitcoin is how the bitcoins themselves are

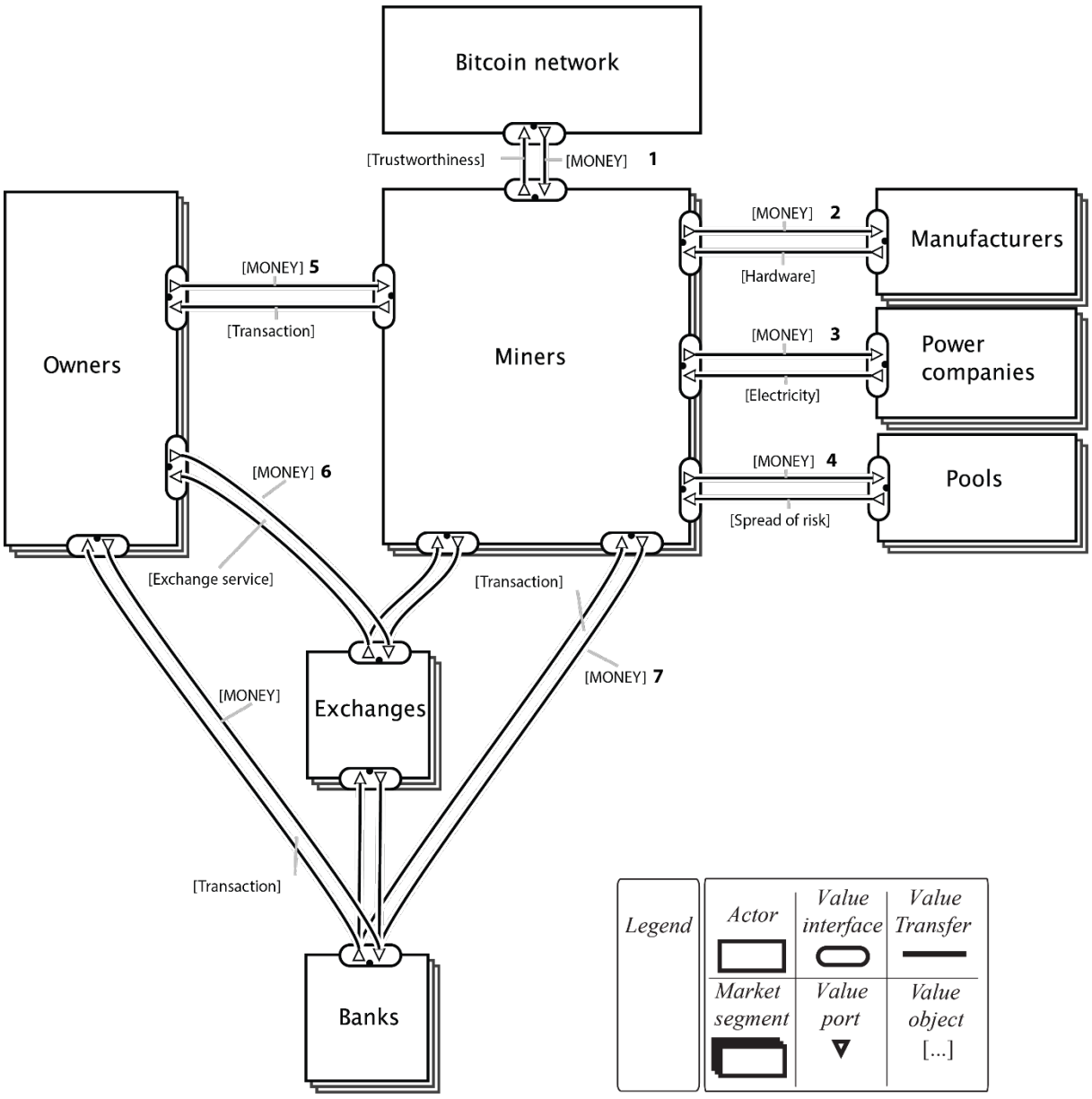

Figure 4: Value flows in the bitcoin network

generated. In traditional currencies (such as the Euro), the central banks play an important role in adding money to the system. In the bitcoin system, money is added to the system by the

system itself. If a miner solves the cryptographic puzzle, a bitcoin is created and assigned to the miner. In the model this is represented by the bitcoin network actor, which reflects the total network of actors.

The central market segment is the conglomerate of miners. Miners have the goal to create a profit, either by mining bitcoins (flow 1) or by collecting a transaction fee (flow 5), paid by bitcoin owners and users using bitcoins for doing transactions. They are crucial for the correct functioning of the blockchain system, as they have approve the blocks with transactions. It is known that miners have serious expenses, most notably for hardware investments and energy. Therefore, we focus our analysis on the miners only, leading to the following research question:

RQ2: Are the miners financially sustainable on the long-term?

Miners are financially sustainable if, on the long term, they can present a positive net cash flows. Apart from their revenues (mined coins and transaction, we need to know their expenses[1]. First, miners have to invest in computing hardware (flow 2). The performance of hardware, which can be used for mining, increases rapidly and becomes more dedicated; Therefore, hardware needs to be replaced (in the order of months, rather than years). Second, they have to pay electricity (flow 3) for the computer they employ. Third, miners often participate in a pool (flow 4). Effectively, participation in a pool increases the chance of revenue in the short term, because once a bitcoin is mined by one of the pool members, the value is divided over the pool participants. Hence, participation reduces the risk of losses in the long term as a result of outdated hardware and consumed electricity. Four, the bitcoin is a

[1] We leave out the costs of internet connectivity, since mining is a very low bandwidth activity. Therefore, internet service providers are not included in the model.

currency that can be kept by the owner, but sometimes participants want to exchange the bitcoin for a regulated currency such as the Euro or the Dollar. For this purpose, there are exchanges, who offer an exchange service for a fee (flow 6). Finally, to interact with a traditional financial system, owners, exchanges, and miners need a bank (e.g. during the use of the aforementioned exchange service). In such a case, a transaction fee has to be paid to the bank (flow 7).

Note that the model abstracts from the flow of bitcoins which are needed for end-user transactions (e.g. to purchase services or goods in return for bitcoins). This follows from our focus on the miners in their value system and not on consumers who use bitcoin for the purchasing of products and services, or speculation. Also, the model leaves out the 'full nodes' that ensure the integrity and safety of the bitcoin network. They are important for the correct functioning of the network, but carry no financial compensation so that monetary flows to those nodes are by definition zero. Moreover, since the number of full nodes is not known at all, it is impossible to include them in the analysis.

We assume that the other actors (e.g. hardware manufacturers and power companies) are capable of generating a positive net cash flow, or can easily be replaced if they go bankrupt. Manufacturers of hardware and electricity power companies have also other customers and can easily calculate the price of their products and service such that a net positive flow results. Pools are a kind of insurance for miners to ensure that, over time, they will have positive revenues. Pools are an effective risk sharing mechanism and base their fees on insurance policies; hence we assume they are capable of generating a positive net cash flow. Similarly, exchanges just trade bitcoins for traditional money. We assume that the losses and profits average over time, and result in a modest net positive cash flow. Although we assume for most actors that they have a net positive cash flow, we nevertheless have to know their cash flow, since miners either

have to pay or receive cash. For example, miners have to pay to the power company a fee for electricity. Below, we briefly introduce how the fees are calculated, which is discussed in more detail in Section 5.

There are a number of money flows to and from the miner, which all have to be quantified:

- Mined bitcoins: Bitcoins obtained as a result of mining. The aggregate information about mining results is publicly available, which is sufficient for the analysis. (value flow 1 of figure 4)
- Hardware investments: these are unknown. In the next section, we present an approach to estimate the installed base of mining hardware over the period of analysis. (value flow 2 of figure 4)
- Electricity expenses: these directly relate to the installed hardware base. For our calculations we assume an average electricity cost of $0.12 per kWh, which is similar to the average cost in the United States.[2] Therefore, once we know which hardware is deployed during which period, we can estimate the total electricity power expenses over time, assuming that mining hardware is always on. Since most hardware is dedicated, this is a realistic assumption. (value flow 3 of figure 4)
- Pool fees: Fees to participate in a pool to spread the risk of mining is approximately 1% of the total coins mined. This is in coherence to the pool Antpool, the largest bitcoin mining pool with a market share of around 25%.[3] (value flow 4 of figure 4)
- Bitcoin transaction fees: from the bitcoin user to the miners whose numbers are publicly available. (value flow 5 of figure 4)
- Exchange fees: we assume an average of 0.5% as they can range from 0.2% to 5% per transaction (Perez, 2015). This is similar to the range of fees exchanges charge per transaction like 0.42% at Kraken.com and 0.5% at bittrex.com[4]. (value flow 6 of figure 4)
- Bank fees: differ per bank and usually contain a fixed and a variable amount. For this research we assume it is similar to the exchange fee with 0.5%. (value flow 7 of figure 4)

Validation of the *e³value* model

[2] Retrieved October 16, 2017, from https://www.ovoenergy.com/guides/energy-guides/average-electricity-prices-kwh.html
[3] Retrieved October 16, 2017, from https://www.buybitcoinworldwide.com/mining/pools/
[4] Retrieved October 16, 2017, from https://en.bitcoin.it/wiki/Comparison_of_exchanges%

The first version of the *e³value* model was presented to the interviewed parties and discussed to obtain feedback in order to validate it. All of the interviewees agreed on the bridging role of banks and exchanges between bitcoin and fiat money. The co-founder of a bitcoin payment provider concluded that while bitcoins are created by the miners, the actual monetary value is assigned once it is sold via exchanges and turned into fiat money via bank accounts. The business manager at a bank noted the scalability of the amount of transactions the bitcoin network can handle is a weakness. The bitcoin consultant underlined the importance of energy prices to mining and predicted a movement toward regions with lower energy prices like China and lower cooling costs like Iceland. The retired bitcoin miner mentioned the centralization occurring with bitcoin mining as the initial investment is increasing continually. The interviewees agreed on the proposed bitcoin value model. One interviewee proposed additional actors that were cost factors for the payment providers, but the interviewee agreed it was not a cost factor to the miners, so these were not added to the model.

After drafting the value model the interviewees were contacted again for comments. The four interviewees had nothing to add. Thus, we consider the e3 value model sufficiently supported by the literature and by the option of experts.

Quantifying value flows

To assess the sustainability of the network, the money flows have to be quantified for actors for which we cannot safely assume a positive net cash flow. As Section 5 explains, we focus on the miner, since the miner is the enabler for the bitcoin system, and has significant expenses (mainly hardware and energy).

For quantification, we rely on publicly available information about bitcoin trade volume, mining revenues, electricity prices, etc. For some data, we have to make estimates. Specifically, the installed mining hardware base is unknown over time but an important cost to actors. We

therefore develop a method to estimate this installed base. The way of estimating is an important contribution of this paper. Finally, we analyze the results for sustainability.

5 Sustainability assessment of the miner

Data collection

Concerning data collection, a significant amount of publicly available data is an advantage of the bitcoin system. In particular, we use data retrieved from blockchain.info, a website that provides daily aggregates of bitcoin creation, transaction volume, transaction fees and network hash rate.

Value flows

For the analysis of sustainability, we first look at the expenses and revenues of miners and the resulting value flows from these. We start by inferring which mining hardware is in use during which specific period. This is necessary as the hardware investment represents a large cash outflow for the miners. Second, each hardware type comes with a different electricity power requirement, influencing the miner's running expenses. Third, the computing performance of specific hardware directly determines the expected number of bitcoins mined by that hardware.

Formally, we solve an equation that models the total bitcoin hash rate on each day as a function of the hardware in operation. From the hardware in operation we can deduce the hardware spending and the electricity costs. Other expenses (pool expenses, bank costs and exchange fees) follow from the total production of bitcoins.

Starting from the observed total bitcoin hash rate, TH_t on day t, it must be the case that

$$TH_t = \sum_{i=1}^{M} HashRate_i \times N_{it} \quad (1)$$

where $HashRate_i$ is the hash rate capability of the hardware of type i, and N_{it} is the number of machines of type i in operation on day t. We have a total of M machines, that are available for purchase over different periods of time (details are below), so we have $N_{it} = 0$ on many days.

We start on $t = 0$ with with a single type of machine, the earliest machine available and set the number of them equal to $TH_t/HashRate_1$. As long as no better type is available, the machines stay in operation to produce the total hash rate that we observe in the data. At a first increase in the hash rate, the number of machines increases to reach the total hash rate. At a decrease in the hash rate, we assume that new machines are throttled back or old machines are turned off [5].

Once a new machine becomes available, we assume that buyers choose between hardware types by picking the machine with the lowest estimated payback time. This way of calculating the attractiveness of an investment is common practice (Berk & DeMarzo, 2014) and the simplicity of the technique fits the dynamism and fast-changing nature of the bitcoin miners. For each machine on the market, the payback time is computed using the 30-day moving average of the bitcoin price:

$$PayBackTime_{it} = HashRate_i \times (P_{\{t,t-30\}} - MC_i)/FC\_i\,, \qquad (2)$$

where MC is the daily marginal cost of running machine i, i.e., the electricity costs, $P_{\{t,t-30\}}$ is the average bitcoin price of the past thirty days (including mining fees) and FC_i is the fixed cost of the machine, i.e., the purchase price. The index-number of the 'best' machine at each time t is i_t^*.

[5] The total network hashrate can fluctuate on a daily basis, but in general it increased by an average of 1.4% per day.

Existing machines stay in operation as long as the marginal profit is positive, i.e., as long as $HashRate_i \times P_t > MC$. If that is not the case, we assume that they are switched off on that day. They can come online again if they become profitable again, for example, when the bitcoin price increases.

The combination of machines in operation on any given day is then simply equal to the number in operation on the previous day, minus machines that have become unprofitable, plus new machines of the type that have the lowest payback time. Let TH_t^{lost} denote the hash rate 'lost' by machines that are switched off because of the profitability condition. Then, we have that

$$N_{it} = \begin{cases} 0 & \text{if } HashRate_i \times P_t < MC \\ \left(TH_t - TH_{t-1} + TH_t^{lost}\right)/HashRate_i & \text{if } i = i_t^* \\ N_{i,t-1} & \text{otherwise,} \end{cases} \quad (3)$$

where $TH_t - TH_{t-1}$ represents the increase in the total hash rate from day $t-1$ to day t that is picked up by new machines coming into operation.

Although the hash rate is increasingly almost continuously in our sample period, there are a few instances where the hash rate declines. We allocate those decreases to the most recent machines that we assume are throttled back proportionally[6]. Since declines in the hash rate are rare and small (see Figure 5 below), we use the most straightforward way of accounting for hash rate declines.

We now turn to the data that is fed into Equations (1) to (3) to determine purchases of new hardware. Figure 5 shows the hash rate and difficulty of the bitcoin network increasing by a factor of more than 347,000 from 2012 to 2016. There are two reasons why this happens. First,

[6] In reality, a decrease in the hash rate could be due to start-up problems of new machines due to overclocking, decommissioning of older hardware, negative price shocks in the value of bitcoin, or alternative use of hardware, for example, to mine other cryptocurrencies.

faster hardware is added to replace slower running hardware for which electricity expenses outnumber mining and transaction revenues. Second, new hardware is added to increase production, as bitcoin mining becomes increasingly popular. In both cases, we attribute the increase in computing power in the bitcoin network to new hardware.

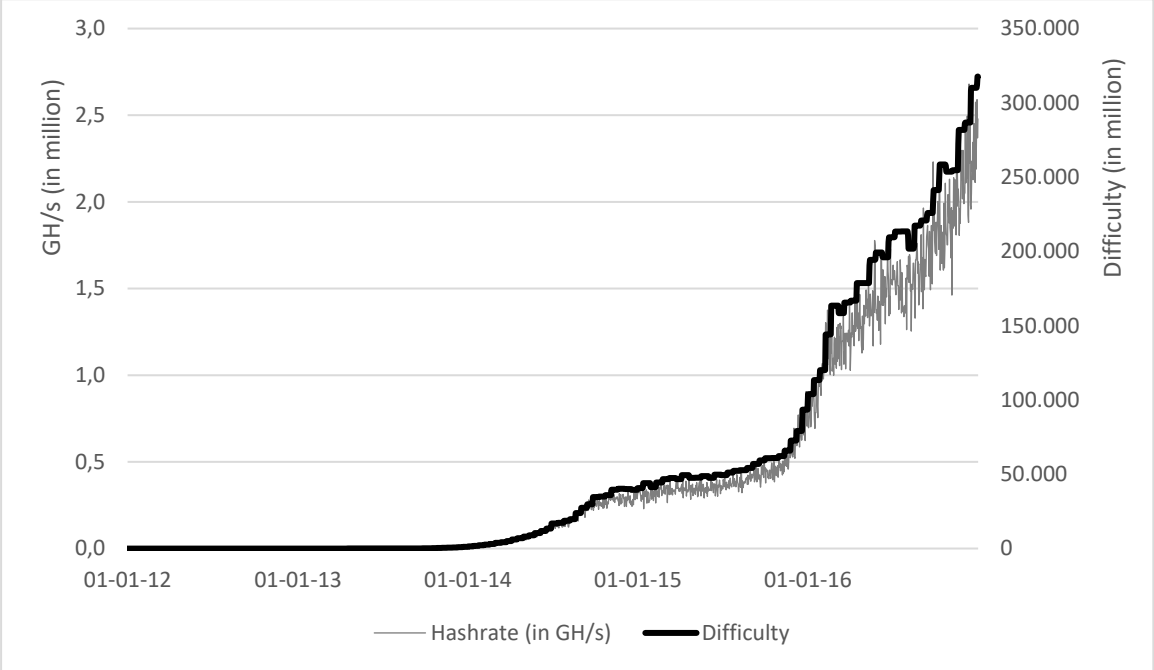

Figure 5: Network hash rate of bitcoin in GH/s and bitcoin difficulty

Source: https://blockchain.info/en/charts/hash-rate & https://blockchain.info/en/charts/difficulty

Value flow: Hardware investments

Regarding the purchasing of mining hardware, we assume that miners behave rationally and therefore buy the hardware with the lowest payback time. The payback time is calculated by taking the upfront investment in mining hardware divided by the average revenue per day (as a result of coins mined plus transaction fees minus energy costs of the preceding 30 days) resulting from that hardware. For each date the most energy-efficient hardware (energy cost per GH/s) compared to the most cost-efficient hardware (amount of computing power per $). Figure

6 shows the comparison between cost-($) and energy-efficient (en.) hardware in 2012. During the year the payback time of the cost-efficient hardware is shorter than that of energy-efficient hardware. The payback time in 2012 could differ from around 82 to 1051 days.

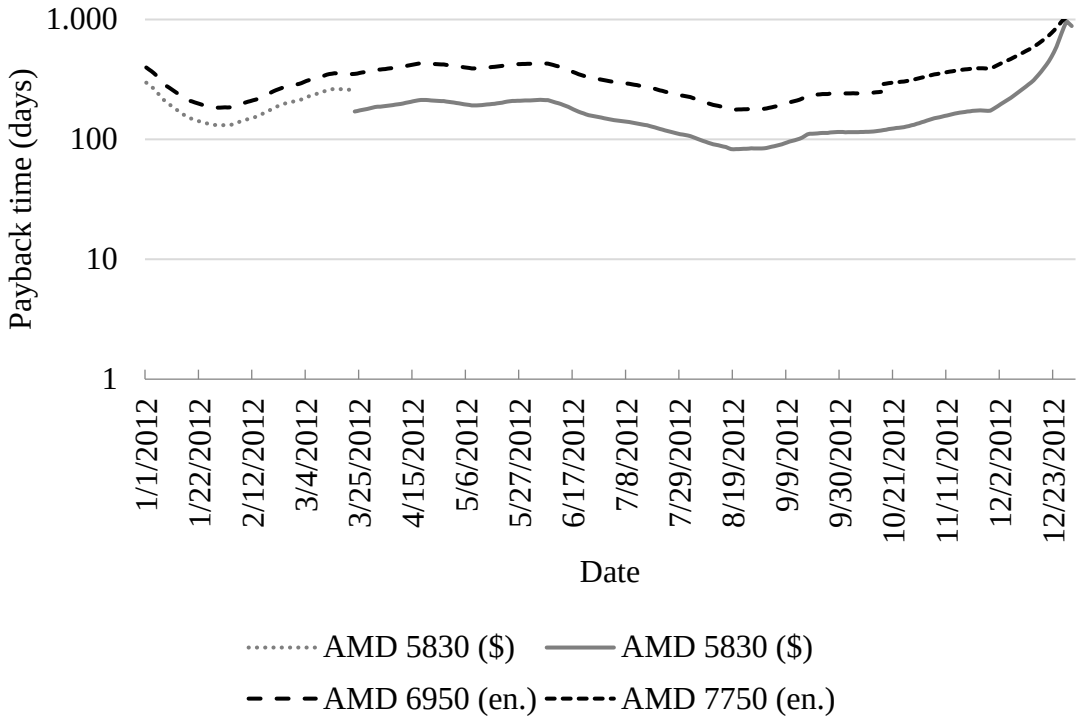

Figure 6: Payback time for most energy-efficient (en.) and cost-efficient ($) hardware.

Source: authors' calculations

Figure 7 shows the estimated payback time for the full period and the revenue per GH/s from 2012 to 2016. The estimated payback time can be as short as three days, but is often between approximately 100 to 300 days. During the first six months of 2016, the payback time is so

high, it would take decennia to earn back the hardware. The payback time in 2012 could range from around 82 to 1051 days.

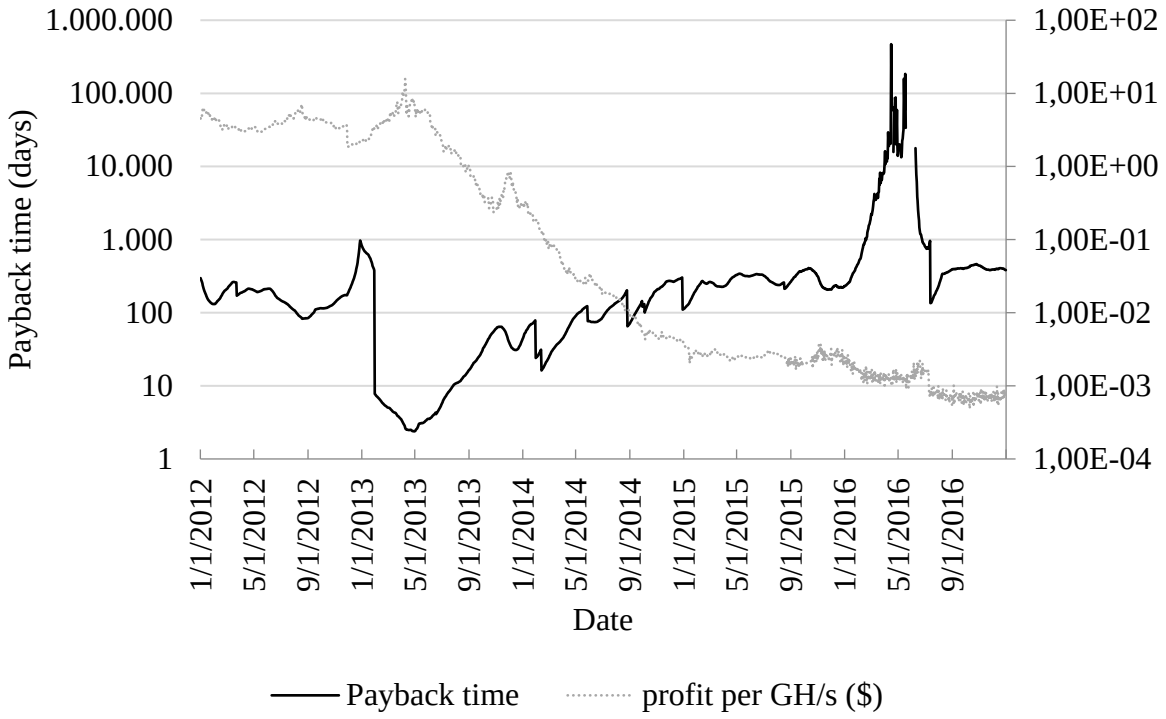

Figure 7: Payback time (days) and revenue per GH/s between 2012 and 2016.

Source: authors' calculations

At the beginning of our analysis period, we assume that the AMD 5830 is installed, which was the best available hardware at that time.

Regarding electricity costs, we use a fixed price of $0.12 per kWh, obtained from ovoenergy.com[7] as the average price across developed countries in our sample period.

Regarding the operation of mining hardware, we assume that mining hardware remains in operation until the daily electricity expenses related to that hardware is equal or higher than the expected revenues for that day, namely the value of the mined bitcoins and the transaction fees.

[7] Retrieved October 16, 2017, from https://www.ovoenergy.com/guides/energy-guides/average-electricity-prices-kwh.html

In other words: after initial investment, the only incentive for miners to turn their hardware off is that the marginal expenses for mining (electricity) outweigh the marginal revenues.

The energy cost for a particular type of hardware is known. The expected number of bitcoins mined per day, as well as the transaction fees for a specific kind of hardware can be derived from the performance indicator (in GH/s) of that hardware. Therefore, in order to calculate the payback period, we must know the expected revenue. To estimate this, we convert the expected number of mined bitcoins to dollars, using the average value of the bitcoin 30 days prior to the investment. This assumes that miners possess no superior timing ability, which seems sensible.

Given the assumptions on purchasing and operations we can estimate the hardware in use over time. As the market of mining hardware is not transparent, the archived pages[8] of a public wiki page[9] are used to select the most cost-effective hardware over the period 2012 to 2016. This data was cross-referenced with discussions on the public forum bitcointalk.org to find the earliest moment new hardware was available to miners. The results are in Table 1.

Since the performance of the bitcoin network is known, we can calculate the upfront hardware investment, if we assume all hardware was the AMD 5830 at that time. Then, for each subsequent day we can infer the hardware purchases using the increase in hash rate and available hardware on that day. With the assumption of positive marginal revenues, we also can calculate when new hardware is added or retired.

Table 1 shows the fast increase of the network's performance rate due to the increasing availability of dedicated hardware for bitcoin mining. Note that, because the hardware is

[8] Collected with the Internet Archive *Wayback Machine* on https://web.archive.org/web/*/https://en.Bitcoin.it/wiki/Mining_hardware_comparison
[9] https://en.Bitcoin.it/wiki/Mining_hardware_comparison

tailored to bitcoin mining, we consider the residual value of hardware zero as it cannot be used economically for other tasks.

Table 1 – Hardware Expenses 2012-2016

#	Hardware	Release date	Hash rate increase (GH/s)	Price range /GH/s (USD)	Total investment (mln USD)
1	AMD 5830	<30-01-13	12,435	463.57-304.64	3.79
2	Avalon 1	30-01-13	127,813	19.59	2.50
3	Avalon 2	18-06-13	121,895	18.28	2.23
4	Block Er. Cube	15-07-13	21,125,418	18.33	387.30
5	Hashfast Sierra	30-01-14	1,429,249	5.90	8.43
6	Coin Terram. IV	12-02-14	65,034,500	3.00	195.07
7	Antminer s1	28-05-14	135,574,060	1.66	225.20
8	ASICM. BE Tube	26-08-14	247,441,781	0.69-0.40	148.72
9	Antminer S4	29-09-14	22,399,375	0.7	15.68
10	Antminer S5	29-12-14	434,622,966	0.32	139.23
11	Antminer S5+	17-08-15	1,776,788,547	0.29	530.83
12	Antminer S9	14-07-16	2,679,978,275	0.17	459.42

Source: authors' calculations

Value flow: Electricity expenses

Now that we know which specific kind of hardware is into operation during which specific period, we can also calculate the electricity consumption of that hardware, and related to that, the electricity expenses. We assume that mining is always running during the period of operation. Table 2 gives the daily expenses for electricity per GH/s for a particular type of hardware, as well as the total electricity expenses for the period the specific hardware was in production.

Table 2 – Energy Expenses 2012-2016

Hardware	Release date	Daily energy costs per GH/s (USD)	Total electricity

#				expenses (mln USD)
1	AMD 5830	<30-01-13	1.7070	5.13
2	Avalon 1	30-01-13	0.0269	1.34
3	Avalon 2	18-06-13	0.0246	1.02
4	Block Er. Cube	15-07-13	0.0192	79.25
5	Hashfast Sierra	30-01-14	0.0025	1.83
6	Coin Terram. IV	12-02-14	0.0032	56.03
7	Antminer s1	28-05-14	0.0058	55.46
8	ASICM. BE Tube	26-08-14	0.0032	72.36
9	Antminer s4	29-09-14	0.0020	19.25
10	Antminer S5	29-12-14	0.0015	240.48
11	Antminer S5+	17-08-15	0.0013	274.51
12	Antminer S9	14-07-16	0.0007	88.48

Source: authors' calculations

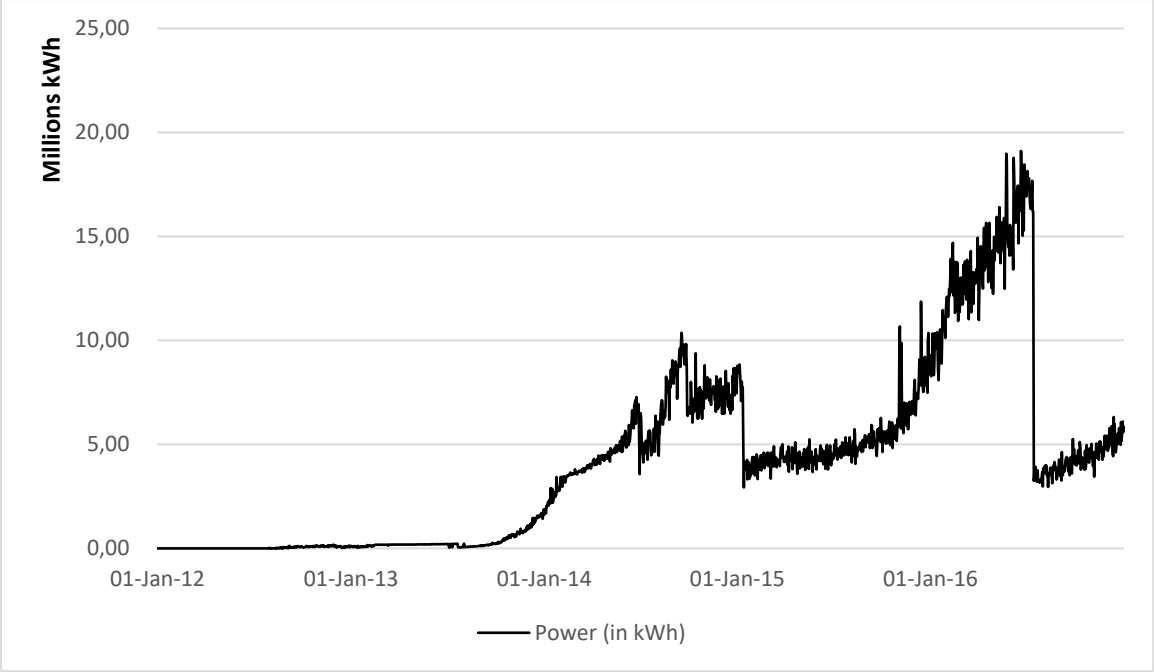

Figure 8: Daily kWh usage of bitcoin network

Figure 8 shows the rapidly increasing energy usage of the bitcoin network from 2014 to 2016. The energy consumption at the peak in 2014, around 5 mln kWh per day, means the bitcoin network is running at around 208 MW. This seems sensible, given the hash rate ultimo 2016 of 2 bln. GH/s and the efficiency of the Antminer S9 which uses 0.1 Joule per GH/s. This translates

to a power use of 200 MW. It does question the earlier estimate of O'Dwyer and Malone (2014), who find a number that is close to the electricity use (3GW) of Ireland in 2014. Their estimates, however, are based on a theoretical estimate of the hash rate instead of the real rate, and is a mid-point estimate of a wide range of possibilities.

Figure 9 gives a graphical representation of our estimates of when certain hardware was in use. The height of the box for a specific kind of hardware indicates the energy expense per GH/s for that hardware. The hardware is phased out as soon as the revenue per GH/s crosses the electricity expense for that hardware (the top-right corner of each rectangle). The sudden drops of profitability during periods like the fourth quarter of 2013 and the second quarter of 2016, suggest the predicted gradual linear and exponential profit declines of online mining calculators are an unreliable tool for net cash flow prediction.

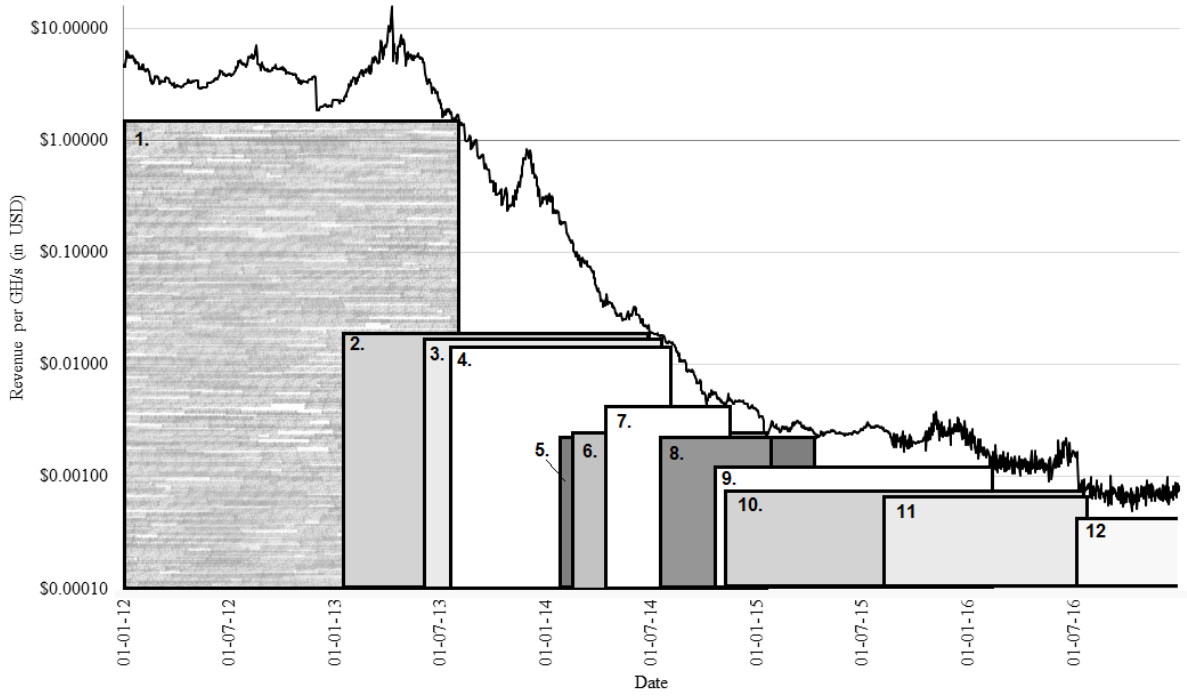

Figure 9: Duration of profitability period per hardware type

Source: authors' calculations

Value flow: other expenses

In order to mine bitcoins, miners will also have expenses to (1) pools, where about two thirds of the miners[10] pay a fee of approximately 1%[11] to a pool owner, (2) 0.5% exchange fees[12] in order to sell bitcoins for regular currencies and (3) 0.5% bank fees are assumed based on the exchange fees. Assuming that all mined bitcoins and earned transaction fees are immediately exchanged for dollars, exchange and bank expenses directly relate to the amount of bitcoins transferred and mined each day. The expenses are summarized in Table 3, by hardware type.

Table 3 – Other Expenses 2012-2016

#	Hardware	Release date	Pool Expenses (mln USD)	Exchange Expenses (mln USD)	Bank Expenses (mln USD)
1	AMD 5830	<30-01-13	0.089	0.067	0.067
2	Avalon 1	30-01-13	0.363	0.273	0.273
3	Avalon 2	18-06-13	0.117	0.088	0.088
4	Block Er.Cube	15-07-13	3.353	2.515	2.515
5	Hashfast Sierra	30-01-14	0.087	0.065	0.065
6	Coin Terram. IV	12-02-14	1.767	1.325	1.325
7	Antminer s1	28-05-14	0.800	0.600	0.600
8	ASICM. BE Tube	26-08-14	0.703	0.527	0.527
9	Antminer S4	29-09-14	0.192	0.144	0.144
10	Antminer S5	29-12-14	2.544	1.908	1.908
11	Antminer S5+	17-08-15	2.018	1.513	1.513
12	Antminer S9	14-07-16	1.487	1.115	1.115

Source: authors' calculations

Value transfers

[10] The 2/3 assumption is based on figures retrieved on June 14, 2016 from https://blockchain.info/pools.

[11] The 1% pool fee assumption is based on figures retrieved on June 14, 2016 from https://en.Bitcoin.it/wiki/Comparison_of_mining_pool

[12] These fees can be as low as 0,2% (0,1% for each trading party) and as high as 5% (Perez, 2015). Since most volume goes through exchanges with a low fee, the average fee is set at 1%..

We now know all components of the miner's expenses and revenues. Table 4 summarizes the expenses and revenues, and calculates per hardware the estimated generated net cash flow. As can be seen from the table, the first part of our analysis period shows a positive net cash flow for miners. The numbers of the flows in table 4 correspond to the numbered value transfers in figure 4. However, the last two periods have a loss. At the end of the measurement period, only the Antminer S9 was still running on a profitable basis, so the losses might be compensated in the later periods. Table 4 also shows that in some time periods the investments in hardware have been very profitable, such as with the Avalon 1 in 2013. The total profits for miners who have used the Avalon 1 in the right time period have been almost $ 50 mln.

Table 4 – Miner Profits per machine 2012-2016

#	Hardware	Release date	Revenues (mln USD)	Expenses (mln USD)	Profits (mln USD)
1	AMD 5830	<30-01-13	13.41	9.28	4.13
2	Avalon 1	30-01-13	54.54	5.30	49.24
3	Avalon 2	18-06-13	17.51	3.71	13.80
4	Block Er, Cube	15-07-13	503.05	479.96	23.08
5	Hashfast Sierra	30-01-14	13.00	10.64	2.37
6	Coin Terram, IV	12-02-14	265.01	258.99	6.02
7	Antminer s1	28-05-14	120.05	283.87	-163.82
8	ASICM, BE Tube	26-08-14	105.47	224.69	-119.22
9	Antminer S4	29-09-14	28.87	36.11	-7.24
10	Antminer S5	29-12-14	381.66	389.89	-8.23
11	Antminer S5+	17-08-15	302.79	813.41	-510.62
12	Antminer S9	14-07-16	223.10	553.11	-330.01*
		TOTAL	2,028.46	3,068.95	-1.040.50

* = Still operational after measurement period

Source: authors' calculations

Table 5 – Value flows of miners in bitcoin network (in mln USD)

#	Value flow	2012	2013	2014	2015	2016	Total
1	Bitcoin mining	2.73	292.14	783.57	372.35	557.16	2,007.95
2	Hardware	-3.79	-208.95	-776.20	-280.01	-849.47	-2,118.42
3	Energy	-1.36	-14.37	-246.24	-227.90	-407.31	-897.18
4	Pool fees	-0.02	-1.96	-5.24	-2.50	-3.81	-13.53
5	Bitcoin fees	0.01	2.12	2.44	2.33	13.61	20.51

6	Exchange fees	-0.01	-1.47	-3.93	-1.87	-2.85	-10.13
7	Bank fees	-0.01	-1.47	-3.93	-1.87	-2.85	-10.13
	Total	**-2.45**	**66.04**	**-249.53**	**-139.47**	**-695.52**	**-1,020.93**
	Average daily net cash flow	**-0.01**	**0.18**	**-0.683**	**-0.382**	**-1.900**	**-0.558**

Source: authors' calculations

Table 5 maps the miner's cash flows to the *e³value* model as introduced in figure 4. Most of the income stems from the generated bitcoins, while most of the costs are due to the hardware investments. The hardware expenses are by far the biggest expense to bitcoin miners. This upfront investment in hardware, combined with a high daily energy cost leads to considerable losses in the later years.

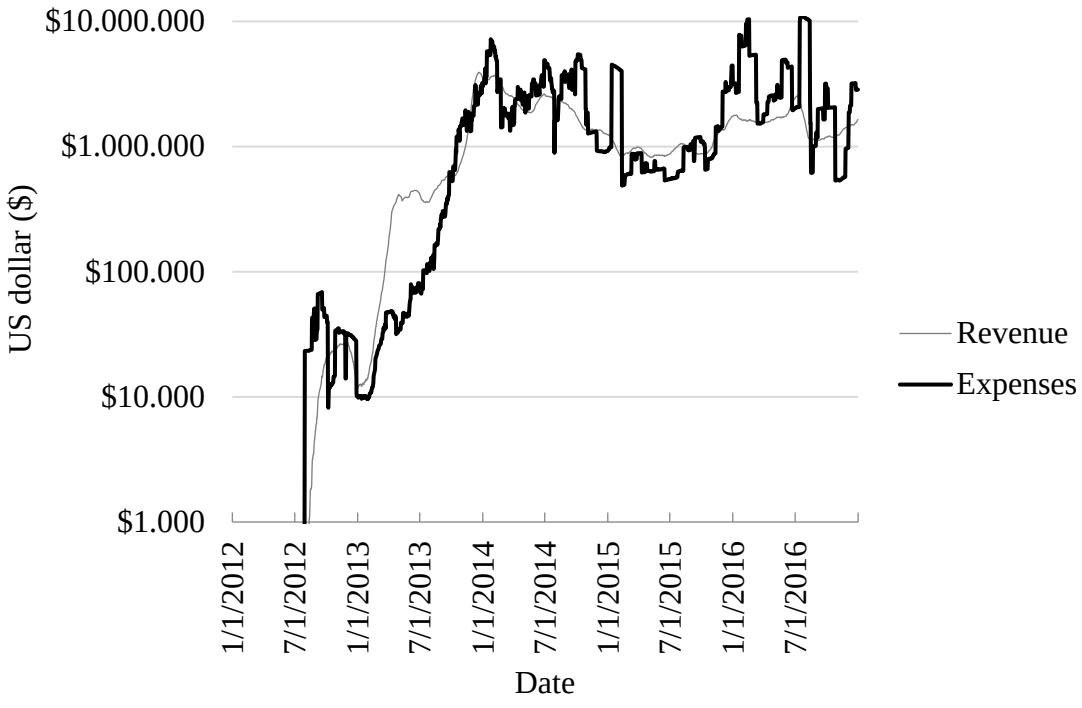

Figure 10: Daily expenses and revenues 30 day average (logarithmic scale)

Source: authors' calculations

Marginal costs

Figure 10 shows the 30-day moving average of total revenues and expenses. As can be seen, the expenses related to bitcoin mining approach the revenues, which is also predicted by economic theory: under full competition, marginal revenue approaches marginal costs. This holds for normal goods as well as for virtual goods and currencies as bitcoin.

Figure 11 shows the marginal expenses (not counting the upfront hardware purchases) compared to marginal revenues. During 2015 and 2016 these lines approach each other, leading to very little profits. This makes it very difficult to have a return on investment on the acquired hardware. The sudden drop in revenue and expenses in mid 2016 is likely a result of the blockchain halving, where the bitcoin reward was halved from 25 to 12.5 per block, and the introduction of a new generation of mining hardware.

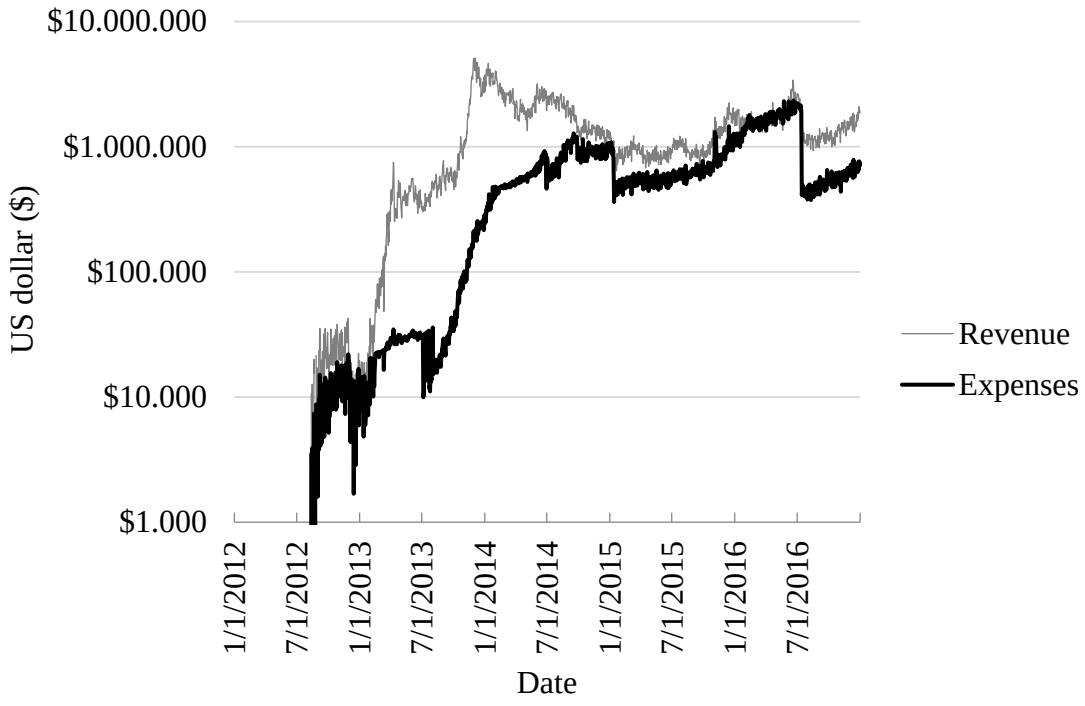

Figure 11: Marginal daily expenses and revenues on a logarithmic scale of 10

Source: authors' calculations

Results

Figure 12 shows the cumulative net cash flow that resulted from Figure 8. Positive flows are followed by periods where money is invested in new hardware, leading to temporarily negative net cash flows. The value of the remaining hardware at the end of the measurement period is $425,040,520.84. By mid-2014, the high revenues of 2012 and 2013 are countered by high expenses, leading to a negative net cash flow from that moment on. It can be seen that this results in a positive net cash flow, but due to necessary new investments, the total net cash flow drops with each innovation. Energy prices determine the profitability of mining hardware, so it could be argued that these prices heavily influence the resulting profits. It is therefore meaningful to do a sensitivity analysis with respect the energy prices. For this purpose, we have also estimated the cumulative profit in scenarios where the energy price is reduced by 50% to $0.06/kWh or reduced by 75% to $0.03/kWh. Figure 10 shows the scenario with an energy price of $0.06/kWh still leads to a negative cumulative cash flow. Only the scenario in which energy is available for $0.03/kWh the bitcoin network is capable of generating a modest positive net cash flow over its complete lifetime.

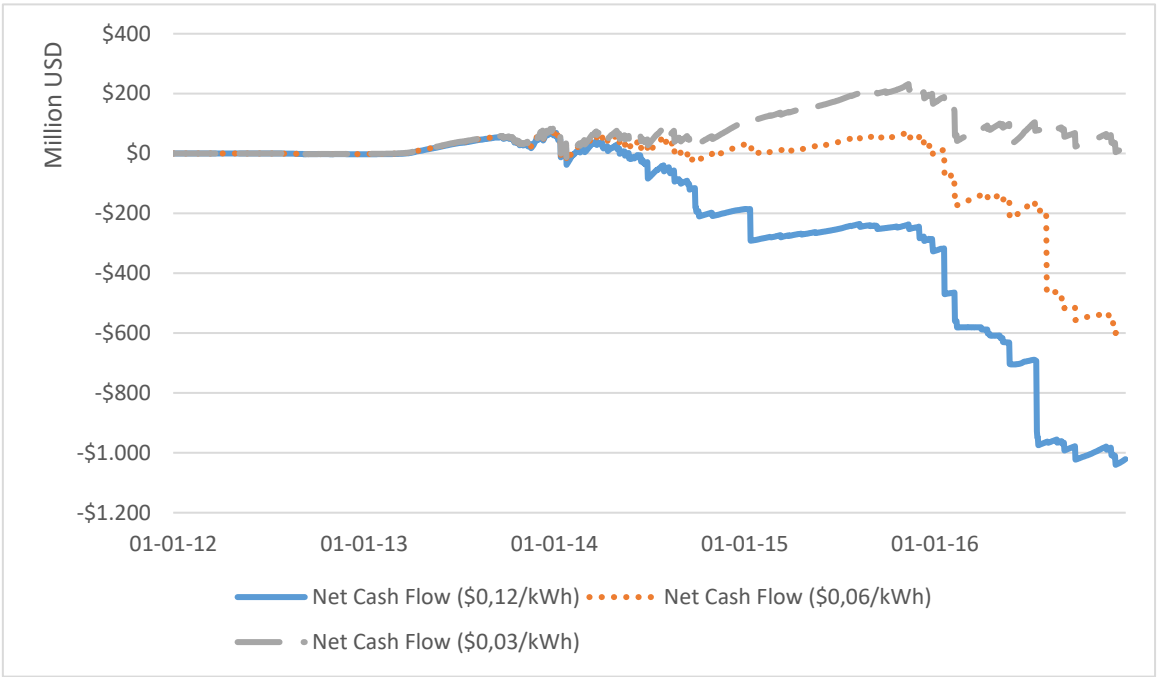

Figure 12: Cumulative net cash flow (in million USD)

Source: Authors' calculations

Reaching the break-even point

A question we can ask is what the exchange rate of the bitcoin should have been in order to reach the break-even point for the modes. This price, as well as the percentage increase/decrease in the exchange rate is given below.

Table 6 – Required break-even price bitcoin for miners from 2012 to 2016 with hardware purchased since 2012

	Bitcoins mined	Net Cash Flow (mln usd)	Average bitcoin price (in usd)	Bitcoin price to break-even (in usd)	Bitcoin price for 20% Profit (in usd)
2012	230,488	-2.45	11.90	22.56 (+89.5%)	27.07 (+107.4%)
2013	1,319,415	66.04	223.02	172.97 (-22.4%)	207.56 (-26.9%)
2014	1,476,412	-249.53	532.38	701.39 (+31.8%)	841.67 (+38.1%)
2015	1,366,223	-139,47	274.25	376.34 (+37.2%)	451.60 (+44.7%)
2016	1,069,366	-695,52	533.74	1,184.16 (+121.9%)	1,420.99 (+146.2%)
Total	**5,461,893**	-1,020.93	**371.38**	**558,31 (+50.3%)**	669.97 (60.4%)

Source: Authors' calculations

The estimates in the above table should be interpreted with care. It is likely to expect that a change in the exchange rate would influence other parameters too, e.g. the number of transactions and the number of miners. Since our analysis is based on factual data of the bitcoin network, we cannot compensate for these effects. To do so, a proper simulation model of the bitcoin network should be developed to include the market dynamics.

6 Discussion

We examined the profitability of proof-of-work bitcoin mining over the period 2012-2016 in the context of the bitcoin's sustainability. An important question is how reliable our estimates are. Our calculation relies on the one hand on publicly available data which are factual (e.g. the bitcoin exchange rate, the number of bitcoins mined, etc.) but on the other hand on an *estimation*

of the installed base of bitcoin mining hardware, as there is not factual data available this. Understanding of the installed base is important, because the kind of hardware installed determines the expenses by miners, namely the initial hardware investment and the expenses for energy. A recent other study by De Vries (2018) also aims to estimate the total energy consumption for the bitcoin, although a different analysis period is used (Feb 10th 2017 – present, see the Bitcoin Energy Consumption Index[13](BECI), which displays the results of their installed base estimate model). In our calculation, at June 20 2016, the electricity power consumption was 19.1 GWh/day, and at December 31rd 2016 5.8 GWh/day (the drop can explained by new, and more energy efficient hardware). The BECI estimates for February 10th 2017 (the first date of analysis) the yearly energy consumption as 9.58 TWh/year, which boils down to 26.24 GWh/day. The difference of 26.24 GWh/day (February 10th 2017) (BECI) 2016 and 5.8 GWh/day (December 31rd 2016) (us) can be explained, apart from the different dates, by the different models used to estimate the installed hardware base. The BECI uses a fairly straightforward model: it assumes that hardware remains in production by miners until it reaches its minimum sales price. Our model supposes a rational behaving miner in the sense that (1) at each point of time, the miner buys the hardware that has the shortest payback time, and (2) the miner takes hardware out of production (and replaces it by newer hardware) if the marginal expenses for mining (electricity) outweigh the marginal revenues. Given the purpose of this paper, namely to argue that the bitcoin network is not sustainable on the long term, our estimate of the installed base is conservative; using the hardware estimation method of the BECI would result in higher energy costs and therefore in increased losses for the miner.

[13] https://digiconomist.net/bitcoin-energy-consumptio

Using our estimation model for the installed base of bitcoin mining hardware we calculated the profits/losses made in the bitcoin's value network and find that marginal profits are converging to the electricity costs of production. This is what economic theory predicts for a market with profit-maximizing companies under full competition. A comparison could be drawn with the value of the Somali shilling between 1991 and 2012. Luther (2015) documents how, in the absence of a central monetary authority, Somali clans produced currency themselves or imported it from foreign producers of paper money. As currency production became a competitive 'industry', the value of the Somali shilling converged to a low but stable currency value that is equal to its intrinsic (paper) value. Similarly, the pattern in Figure 8 suggests that bitcoin mining has become a competitive industry.

At the end of our sample period, profits become negative, even with energy prices as low as $0.06/kWh. Given that bitcoins can be mined by everyone and everywhere, this is a direct result of the competitive pressure on mining bitcoins. Once hardware has been purchased, it becomes a sunk cost and only the marginal costs need to be covered. At the same time, the operators of mining hardware need to make an *average* profit over the lifetime of the hardware, taking into account the wildly fluctuating prices of bitcoin. This makes them reluctant to switch off the hardware, even at very low rates of profitability. Actual loss-making operations are of course irrational, but could reflect the fact that a sizeable fraction of miners in the bitcoin industry are not financially literate and might underestimate the electricity costs that they are incurring, for example.

There are a number of ways how the bitcoin can be made economically sustainable. Unfortunately, none of these possibilities are very realistic. First, the energy price could drop significantly world-wide, for example to 0.03 USD/KWh. Then there would a slight profit for the miners. But even in Inner Mongolia, which is considered to have one of the lowest energy

prices (0.04 USD/KWh, Peck, M.E. (2017)), the long term profitability for miners is doubtful. Additionally, reducing energy consumption use could be achieved by introducing predefined and trustful parties to operate the consensus mechanism (and the release of additional coins), which can be done in a far more energy-efficient way. Although this contradicts the design philosophy of the bitcoin somewhat, i.e., to be independent of a central authority, it does point to a potential future for banks as providers of efficient consensus mechanisms for transactions of electronic money. Finally, a more efficient consensus mechanism could be used, including proof-of-stake (consensus should only be reached by parties who own the most bitcoins, since they have the most interests in trust in the currency (Narayanan, 2016)), Byzantine fault tolerance (a voting mechanism in distributed systems, e.g. Bitcoin-NG (Eyal et al., 2016)), or approaches to filter diverging traffic (e.g. Sieve, as used in Hyperledger (Cachin, 2016; Cachin et al., 2016)). However, other limitations and hurdles to the acceptance of bitcoin as an efficient payment mechanism will remain. For example, it is not clear whether any distributed ledger mechanism could rule out multiple equilibria, (Biais et al., 2017). Also, some consensus mechanism (e.g. Byzantine fault tolerance) do not scale to millions of users.

Second, the bitcoin price may increase substantially, which happened in 2018, which however outside our analysis period. The recent history however has shown that the bitcoin exchange rate is very volatile. Actually, bitcoin is nowadays used as a very high risk speculation instrument, rather than a payment instrument. Therefore, speculating on the increase of the bitcoin exchange rate is very risky, and therefore not reliable enough to justify long-term economic sustainability.

Third, another solution might be to increase the transaction fees that miners get if they include transactions in the blockchain. However, if we take the numbers of 2016 for example, the transaction should be increased dramatically: the earnings from transactions fees were 13.61

million USD, whereas the mining earnings were 557.16 million USD. In other words, the income for transaction clearing is neglectable compared to mining. Moreover, a substantial raise of the transaction fees would change the business model of the bitcoin significantly: from neglectable transaction costs to high transaction costs.

Finally, it can be doubted whether the bitcoin is a significant and desirable payment solution at all, compared to traditional payments as offered as banks. Take for example the transaction volume of VISA[14] alone, which is 141 *billion* transactions in 2016. In that same year, the bitcoin platform processed about 83 *million* transactions[15]. This implies that the bitcoin is neglectable as it comes to the world wide transaction volume. Moreover VISA spent about 0,187 TWh to process their 141 billion transactions (1,3 Wh per transaction) whereas bitcoin, based on our estimation of the installed base, needed 3,39 TWh (41 KWh per transaction) for 83 million transactions.

7 Conclusion

This paper analyzed the long term financial sustainability of proof-of-work mining for the bitcoin network. We have considered the profitability of the miner, expressed by a sustainable net positive cash flow, as the key factor in judging bitcoin sustainability. By reverse-engineering the type and number of computers that have been mining bitcoin, we found a negative net cash flow for most of the measurement period. This answers research question 2: on the long term, miners can not be sustainable. Since the miners are crucial for the correct

[14]https://usa.visa.com/dam/VCOM/download/corporate-responsibility/visa-2016-corporate-responsibility-report.pdf
[15] https://www.quandl.com/data/BCHAIN/NTRAN-Bitcoin-Number-of-Transactions

functioning of the bitcoin network, this endangers the sustainability of the bitcoin network itself (research question 1).

In terms of future research, an important question is how to build a payment service that is (1) economically sustainable, and (2) can scale up to transaction volumes handled by the traditional banks, and (3) fully decentralized, that is, without any intermediate party such as banks.

A key component of the answer is a consensus mechanism that is very scalable and economically sustainable. Clearly, Proof-of-work is not economically sustainable, as argued in this paper. Finding such a consensus mechanism is ongoing work, although important steps are taken. One example is the Proof-of-elapsed-time (PoET) mechanism such as implemented in Hyperledger. PoET claims to be highly scalable and energy friendly.

References

Alt, R., & Puschmann, T. (2012). The rise of customer-oriented banking-electronic markets are paving the way for change in the financial industry. *Electronic Markets*, 22(4), 203-215.

Biais, B., C. Bisière, M. Bouvard and C. Casamatta (2017). The Blockchain Folk Theorem. *Working paper TSE-817*, Toulouse School of Economics.

Barber, S., Boyen, X., Shi, E., Uzun, E. (2012). Bitter to Better - How to Make bitcoin a Better Currency. In Keromytis, Angelos D. (Eds.), *Financial Cryptography and Data Security: 16th International Conference*. pp. 399-414). Springer Berlin

Berk, J. and P. DeMarzo (2014) *Corporate Finance.* Third and Global Edition. Pearson.

Bouoiyour, J., & Selmi, R. (2015). What does Bitcoin look like?. Annals of Economics & Finance, 16(2).

Cachin, C., Schubert, S. and Vukolic, M. (2016), Non-determinism in Byzantine Fault-Tolerant Replication, *ArXiv e-prints*, 1603.07351

Cachin, C (2016). Architecture of the Hyperledger blockchain fabric.,*Mimeo, IBM Research - Zurich*

Chen, C. (2015, January 9). Bitcoin exchange Bitstamp is back online with multi-sig security after hack. *Cryptocoinsnews* Retrieved from https://www.cryptocoinsnews.com/bitcoin-exchange-bitstamp-is-back-with-multi-sig-security-after-hack/

Courtois, N. T., Grajek, M., & Naik, R. (2013). The Unreasonable Fundamental Incertitudes Behind bitcoin Mining. *arXiv preprint arXiv:1310.7935*.

Davies, S. (2015) bitcoin company Coinbase lands $75m investment from NYSE and BBVA. *Financial Times*, January 20, 2015.

Decker, C., & Wattenhofer, R. (2015). A fast and scalable payment network with bitcoin duplex micropayment channels. In: *Symposium on Self-Stabilizing Systems* (pp. 3-18). Springer International Publishing.

Edgar Fernandes, N. (2014, December 3) Pantera Capital leads $3.5m investment in bitcoin microtransaction service Changetip. *Cryptocoinsnews,* Retrieved from https://www.cryptocoinsnews.com/pantera-capital-leads-3-5m-investment-bitcoin-microtransaction-service-changetip/

Ember, S. (2015). Jitters After bitcoin Exchange Suspends Services. *The New York Times,January 5, 2015* Retrieved from http://dealbook.nytimes.com/2015/01/06/jitters-after-bitcoin-exchange-suspends-services/

European Central Bank (2015). Virtual currency schemes – a further analysis. Retrieved from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

Eurostat. (2016, June). Electricity production, consumption and market overview. Retrieved May 15, 2017, from http://ec.europa.eu/eurostat/statistics-explained/index.php/Electricity_production,_consumption_and_market_overview

Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). Bitcoin-ng: A scalable blockchain protocol. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)* (pp. 45-59). USENIX Association.

Forte, P., Romano, D., & Schmid, G. (2016). Beyond Bitcoin--Part II: Blockchain-based systems without mining, *Cryptology ePrint Archive* 2016-747.

Gervais, A., Capkun, S., Karame, G. O., & Gruber, D. (2014). On the privacy provisions of bloom filters in lightweight bitcoin clients. In Proceedings of the 30th Annual Computer Security Applications Conference (pp. 326-335). ACM.

Gordijn, J., & Akkermans, J. M. (2003). Value-based requirements engineering: exploring innovative e-commerce ideas. *Requirements engineering*, *8*(2), 114-134.Grinberg, R. (2012). bitcoin: an innovative alternative digital currency. Hastings Sci. & Tech. LJ, 4, 159.

Higgins, S. (2015, January 12). CEX.io halts cloud mining service due to low bitcoin price. *Coindesk*, Retrieved from http://www.coindesk.com/cex-io-halts-cloud-mining-service-due-low-bitcoin-price/

Holbrook, M. B. (1999). *Consumer Value: A Framework for Analysis and Research*, Routledge, New York, NY

Luther, W.J. (2015). The monetary mechanism of stateless Somalia, *Public Choice*, 165, pp. 45-58.

Moore, T.,Christin, N. (2013). Beware the Middleman: Empirical Analysis of bitcoin-Exchange Risk. In Sadeghi, Ahmad-Reza (Ed.), Book Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers. pp. 25-33). Springer Berlin

Möser, M., & Böhme, R. (2015, January). Trends, tips, tolls: A longitudinal study of bitcoin transaction fees. In International Conference on Financial Cryptography and Data Security (pp. 19-33). Springer Berlin Heidelberg.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Consulted*, *1*(2012), 28.

Narayanan, B. F. (2016). *Bitcoin and cryptocurrency technologies*. Princeton: Princeton University Press.

Normann, R. & Ramirez, R. (1994). *Designing Interactive Strategy - From Value Chain to Value Constellation*, John Wiley & Sons Inc., Chichester, UK.

O'Dwyer, K. J., & Malone, D. (2014). Bitcoin mining and its energy footprint. In: Proceedings of the 25th Joint IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). IET, pp. 280-285.

Peck, M.E. (2017) Why the Biggest Bitcoin Mines Are in China. https://spectrum.ieee.org/computing/networks/why-the-biggest-bitcoin-mines-are-in-china

Perez, Y. B. (2015, February 24). Bucks to bitcoin: Top exchange platform fees compared, *Coindesk*, Retrieved from http://www.coindesk.com/bucks-to-bitcoin-top-exchange-platform-fees-compared/

Porter, M. E. (1985). *Competitive Advantage - Creating and Sustaining Superior Performance*, Free Press, New York, NY

Tapscott, D., Ticoll, D. & Lowy, A. (2000). *Digital Capital - Harnessing the Power of Business Webs*, Nicholas Brealy Publishing, London, UK.

Yardeni, E. & Abott, J. (2015). Stock Market Briefing: S&P 500 Profit Margins, Sectors & Industries. Yardeni Research, Inc. Retrieved from www.yardeni.com

Yermack, D. (2013). Is bitcoin a real currency? An economic appraisal, *NBER Working Paper no.* 19747. National Bureau of Economic Research.

Vries de, A. (2018). Bitcoin's Growing Energy Problem, *Joule*, pp 808-809, Elsevier