Available online at www.sciencedirect.com

ScienceDirect

Current Opinion in Environmental Sustainability

Sustainability of bitcoin and blockchains

Harald Vranken[1,2]

Bitcoin is an electronic currency that has become increasingly popular since its introduction in 2008. Transactions in the bitcoin system are stored in a public transaction ledger ('the blockchain'), which is stored in a decentralized, peer-to-peer network. Bitcoin provides decentralized currency issuance and transaction clearance. The security of the blockchain depends on a compute-intensive algorithm for bitcoin mining, which prevents double spending of bitcoins and tampering with confirmed transactions. This 'proof-of-work' algorithm is energy demanding. How much energy is actually consumed, is subject of debate. We argue that this energy consumption currently is in the range of 100–500 MW. We discuss the developments in bitcoin mining hardware. We also briefly outline alternative schemes that are less energy demanding. We finally look at other blockchain applications, and argue that also here energy consumption is not of primary concern.

Addresses
[1] Open University of the Netherlands, P.O. Box 2960, 6401 DL Heerlen, The Netherlands
[2] Radboud University, P.O. Box 9010, 6500 GL Nijmegen, The Netherlands

Corresponding author: Vranken, Harald (harald.vranken@ou.nl)

Current Opinion in Environmental Sustainability 2017, **28**:xx-yy

This review comes from a themed issue on **Sustainability governance and transformation**

Edited by **Carolien Kroeze**, **Harald Vranken**, **Marjolein Caniels** and **Dave Huitema**

Received: 10 February 2017; Accepted: 23 April 2017

http://dx.doi.org/10.1016/j.cosust.2017.04.011

Introduction

People have been using currencies for thousands of years. Initially, currencies were minted directly from precious metals such as gold and silver. Later on, paper money was introduced and the face value of cash was decoupled from its nominal value, but currencies were still backed up by gold depositories. Nowadays, fiat currencies are allowed to float freely, only backed up by the faith and credit of the states that issue them. Bitcoin is a decentralized system that attempts to overcome the weaknesses of fiat and gold-based currencies. It is not governed by central authorities, such as governments or central banks, and intermediaries for currency issuance or settlement and validation of transactions, and can provide lower transaction fees for payments [1,2]. The Bitcoin Foundation provides some centralized governance for standardization, protection and promotion of bitcoin, but it does not act as a central bank and does not issue currency [3].

Bitcoin was introduced in 2008 by Satoshi Nakamoto [4], which is a pseudonym of an author or group of authors whose identity is covered in mysteries. The term 'Bitcoin' often refers to the system, while the term 'bitcoin' or BTC refers to the unit of currency. In this paper, for simplicity we just use the term bitcoin. Bitcoin is an electronic, virtual currency that has no physical representation such as coins or banknotes. The bitcoin ecosystem is a network of users that communicate with each other using the bitcoin protocol via the Internet. The bitcoin protocol is available as an open source software application and allows users to store and transfer bitcoins for purchasing and selling goods, or to exchange bitcoins for other currencies. The issuance of bitcoins takes places in the network while handling transactions in a process called bitcoin mining. The bitcoin network started in 2009 and ever since bitcoin has been the most popular decentralized currency. In January 2017 there were 16 million bitcoins in circulation with a total value of roughly 16 billion US dollars, although the exchange rate of bitcoins has shown very large fluctuations.

Both scientific and professional literature on digital currencies, with bitcoin as prime example, is extensive. Some provide gentle, general introductions to the technology applied in bitcoin (e.g. [5]), while others provide more detailed overviews of the technical operation of bitcoin (e.g. [6•,7•,8]) as well as economical and financial aspects (e.g. [9•]).

In this review paper we provide an overview and synthesis of recent literature published in the last two years that addresses the sustainability of bitcoin. The sustainability of bitcoin is depending on a mix of environmental [10••,11••], economical [1,12], financial [2,13,14] and ethical [15] aspects. Bitcoin may pose risks to the stability of the current financial system, while also lack of controls over bitcoin exchanges and the volatility of the bitcoin currency raises concerns. Our focus in this review is on sustainability in the context of environmental and economical aspects. We try to answer the question whether the bitcoin system is sustainable given the energy consumption required for bitcoin mining, which has been

subject of debate in the last few years. The contributions of this paper are: firstly, to synthesize and critically assess the viewpoints in scientific literature; and finally, to argue that the energy consumption of the bitcoin system is not excessive, which stands in contrast to the public opinion that bitcoin mining is a gross waste of energy. We explore four subquestions: What factors play a role in the energy consumption of bitcoin mining, how large is this energy consumption, does this impede sustainability, and if so are there alternatives that can reduce energy consumption? In the following sections we outline the basic operation of the bitcoin system, we summarize trends in the hardware used for bitcoin mining, we discuss the energy footprint of bitcoin mining, we present some of the alternatives that have been proposed to reduce energy consumption, and we briefly discuss other applications of the blockchain technology that is at the basis of the bitcoin system.

Overview of the bitcoin system

The bitcoin system is a distributed, peer-to-peer network. There is no central server or point of control, and all nodes in the network are equal peers. Each transaction to transfer an amount of bitcoins among users is transmitted to the bitcoin network where it is stored in a distributed transaction ledger, the blockchain. The blockchain contains the entire history of bitcoin transactions. Each node in the network stores a (complete or partial) copy of the blockchain. New transactions are propagated rapidly across the nodes in the network. A transaction is in fact a transfer from a source of funds (called an input) to a destination (called an output). Transaction inputs and outputs are not related to accounts or balances: an input is a reference to an unspent transaction output of the sender in a previous transaction. Before forwarding a transaction to its neighbors, each node first verifies the transaction, which includes checking the syntax and structure, and whether it is a valid transfer of an amount of yet unspent transaction outputs. Each node independently verifies the transactions received, propagates valid transactions, and builds a pool of valid transactions. The valid transactions are added to the blockchain in a process called bitcoin mining. Each node collects a number of valid transactions into a block and tries to compute a cryptographic hash of the block that meets certain constraints (based on the ideas of Hashcash [16]). A cryptographic hash is a kind of checksum for the block, that is one-way (meaning that it is easy to compute a hash of a given block, but difficult to compute a block that matches a given hash) and collision resistant (meaning that it is difficult to find two blocks that yield the same hash). Finding a hash that meets the constraints imposed by the bitcoin system, is a compute-intensive task that can be executed only by brute-force trying. This implies a race among the nodes in the network to find a valid hash as quickly as possible. The first node that finds such a hash, wins the block, which means that this block is added to the blockchain and propagated to the network. Although computing a valid hash is difficult, verifying whether a hash is valid is easy and hence each node that receives the block can quickly identify whether the new block is valid. When a node receives a new valid block, it stops the mining process for the current block and starts mining for a new block. The node that won the block receives a block reward, which is a fixed amount of new bitcoins. Hence, the issuance of bitcoins (minting) is done during the bitcoin mining process. The node that won the block also receives the transaction fees for every transaction included in the block. Every 10 min on average, a node is able to mine a new block. It can be the case that multiple nodes simultaneously generate a valid block, which causes that multiple versions of the blockchain ('forks') occur temporarily. Forks are resolved as soon as one of the forks contains more blocks. The computations to find and verify a cryptographic hash of a block during bitcoin mining allows the bitcoin network to gain consensus about the state of transactions. This elegantly solves the issue of double spending and hence an amount of bitcoins cannot be spent twice. The bitcoin mining process decentralizes the currency issuance and the transaction clearing normally done by central banks and clearinghouses. In economics bitcoin is considered as money to some extent, since it offers a unit of account, means of payment, and store of value [1,3]. It can even be argued that bitcoin has an intrinsic value due to the computational effort for bitcoin mining [17].

Each block does not only contain transactions, but also the hash of the previously accepted block in the blockchain. Hence, the blocks in the blockchain are linked to each other: they form a chain of blocks, thence the term 'blockchain'. This provides security, as a node with malicious intent cannot easily replace or modify an already accepted transaction or add a new transaction to an already accepted block, since this would require to redo the computations to find a valid hash for the modified block. And since new blocks are continuously added to the blockchain, each block linking to the previous block, also the hashes of the newly added blocks would have to be recomputed.

The initial block reward was set to 50 BTC. The reward is halved every 210 000 blocks, which is approximately every four years. This will continue until 2140 when the mining reward drops below 10^{-8} BTC, which is the minimal unit of bitcoin also known as satoshi. Afterwards, transaction fees will provide the necessary incentive to continue mining of new blocks [18]. The bitcoin protocol includes an algorithm to regulate that on average every 10 min a new block is mined, by adjusting the difficulty to find a valid hash. This is required to keep up with the improvements in the performance of mining hardware which allows bitcoin miners to compute more and more hashes per second.

Hardware for bitcoin mining

Bitcoin mining is attractive since it offers a strong financial incentive. For each block mined, the miner receives a block reward as well as the transaction fees of the transactions in the block. As bitcoin gained in popularity, an arms race started among miners. Bitcoin miners initially used general-purpose computers, but they quickly switched to more dedicated hardware that offered higher performance (in terms of hash rate R, measured in the number of hashes (h) computed per second) at lower energy costs (in terms of energy efficiency E, measured in the number of hashes computed per Joule). This dedicated hardware for bitcoin mining has developed in a remarkable way, and bitcoin miners even self-financed hardware and software development [19••,20].

The bitcoin mining hardware has seen four generations [19••,20,17], see Table 1. Initially miners used general-purpose computers, in which the actual computations are performed by the Central Processing Unit (CPU). Although modern CPUs can execute software with a certain amount of parallelism, and multiple threads can be executed in parallel on multicore CPUs, they are not optimized for bitcoin mining. This first generation of bitcoin mining hardware using CPUs, is the least powerful and the least energy efficient. As the difficulty of mining increased, the operational costs of CPUs exceeded the profits from mining.

The second generation occurred at the end of 2010 when bitcoin miners started to use the Graphics Processing Unit (GPU) in the graphics cards of their computers. These GPUs are designed to perform complex graphics calculations with lots of parallelism, which can be used efficiently for bitcoin mining. GPUs offered higher hash rates and better energy efficiency than CPUs.

As the use of GPUs became more widespread, bitcoin miners started to look for more powerful and more efficient alternatives. The third generation occurred mid 2011 when miners switched to Field Programmable Gate Arrays (FPGAs). The circuits in an FPGA can be configured and programmed by users after manufacturing. Bitcoin miners customized FPGAs to support mining, which allowed to increase hash rates even further at lower power consumption. The popularity of FPGAs was brief, since the fourth generation appeared quickly.

Table 1

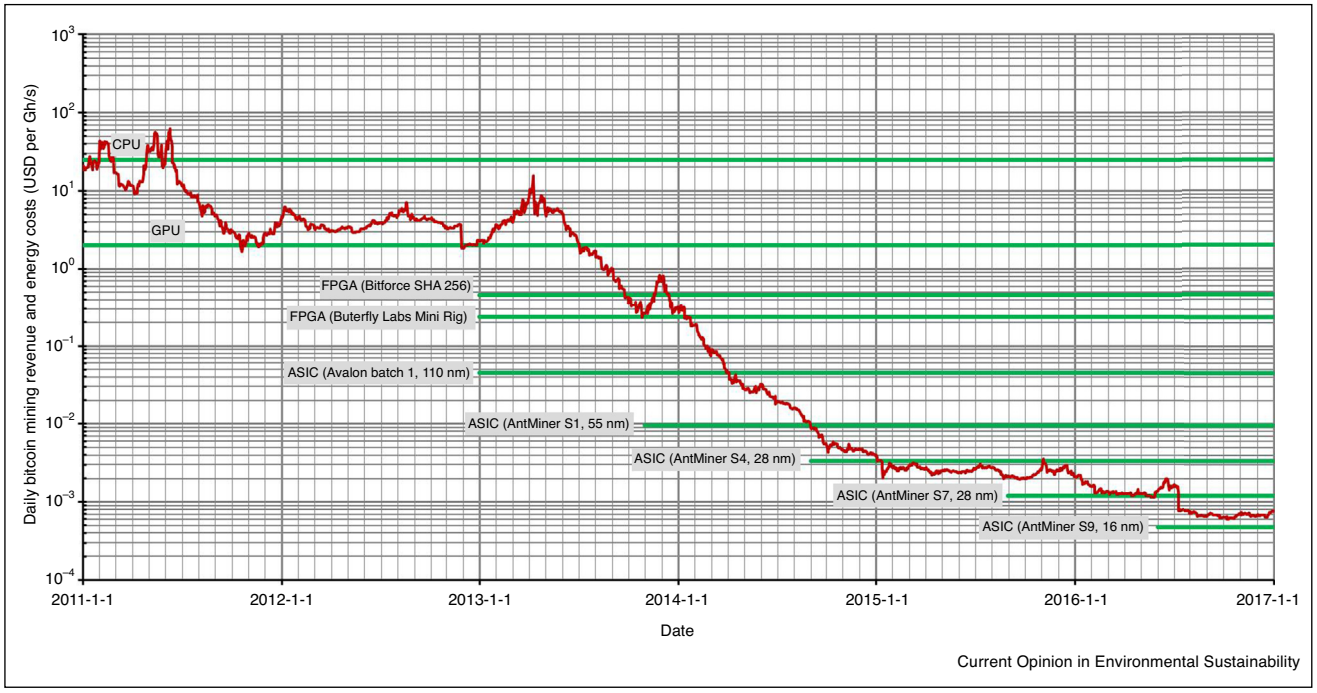
Hash rate and energy efficiency (orders of magnitude) of four generations of bitcoin mining hardware (data source: en.bitcoin.it/wiki/mining_hardware_comparison)

Hardware	Introduction	Hash rate (h/s)	Energy efficiency (h/J)
CPU	2009	10^5–10^8	10^4–10^5
GPU	Late 2010	10^6–10^9	10^5–10^6
FPGA	Mid 2011	10^8–10^{10}	10^7
ASIC	Early 2013	10^{10}–10^{13}	10^8–10^{10}

The fourth generation appeared early 2013 with the introduction of Application-Specific Integrated Circuits (ASICs) containing dedicated circuitry that is optimized to perform hashing computations as efficiently as possible. Butterfly Labs, ASICMiner and Avalon were the first companies that provided ASICs for bitcoin mining, financed by online presales. ASICMiner initially did not ship ASICs to customers, but ran the ASICs in their own data center, which allowed them to capture a large fraction of the total network hash rate. These first ASIC manufacturers were very successful. Other companies with greater capitalization quickly followed and developed the next generations of ASICs with improved technology. Currently, the most advanced technologies are only utilized by chip manufacturers that run their ASICs in their own data centers located in areas that have low-cost energy and cooling. The bitcoin mining industry is however very competitive. For instance, the Swedish company KnCminer operated data centers located in the Arctic circle to benefit from locally sourced hydroelectric power and cool air at extremely low cost, but still went bankrupt mid 2016. Many large miners are located near cheap sources of electricity, such as hydroelectric dams (China, Republic of Georgia) and geothermal power plants (Iceland).

Figure 1 shows the daily revenue in US dollars per Gh/s earned by bitcoin miners in the period 2011–2016. The figure combines historical data on the mining revenue (i.e. block rewards and transaction fees) and the hash rate of the bitcoin network with US dollar to BTC exchange rate. The drops at the end of 2012 and mid 2016 correspond to the transition of the block reward from 50 BTC to 25 BTC and from 25 BTC to 12.5 BTC. The horizontal lines show the estimated daily energy cost per Gh/s for CPUs, GPUs, and a number of FPGAs and ASICs, including five generations of ASICs in Bitmain's Antminer product line. Bitmain Technologies, founded in 2013, is currently one of the leading ASIC manufacturers that ship ASICs to customers. When the revenue of mining drops below these costs, profit turns negative and miners have to switch to more efficient hardware [21]. Note that this figure is in line with the analysis by Taylor [19••] and shows costs for hardware that can be purchased by private customers and run at electricity costs of 200 USD/MWh. Electricity costs however vary widely in different countries, and even within countries, depending on infrastructure and geography. For instance, in 2015 the electricity prices in OECD countries ranged for consumers from 75.33 USD/MWh in Mexico to 337.38 USD/MWh in Denmark, and for industry from 35.34 USD/MWh in Norway to 263.33 USD/MWh in Italy (source: International Energy Agency, www.iea.org). Industrial users run purpose-built data centers comprised of specialized

Figure 1



Daily mining revenue and daily mining energy cost for different types of hardware (USD per Gh/s) (data sources: www.blockchain.info for daily mining revenue; en.bitcoin.it/wiki/mining_hardware_comparison for energy costs).

servers that integrate arrays of ASICs ('ASIC clouds') offering better performance and energy efficiency [20].

Bitcoin miners did not only participate in grass-root efforts to produce efficient hardware, they also cooperate in mining pools in which participants split up the computations to mine a block. If a block is mined, each participant is rewarded according to their contribution.

The bitcoin arms race increases the capital expenditure, which throws up barriers for newcomers to enter and causes miners that cannot keep up to drop out. This leads to an oligopolistic market. According to data from bitcoinchain.com, the five largest miners, which are mostly based in China, mined over 85% of the blocks in 2016. This implies several risks, such as government interventions and undermining bitcoin's principle of a decentralized currency.

An interesting question is how bitcoin mining ASICs will evolve in the near future. The semiconductor industry has been introducing new CMOS process technology generations at a fairly constant two-year pace [22]. With each new generation, the dimensions of transistors on chips are scaled down further by a factor S, which typically is $\sqrt{2}$. According to Dennard's classic scaling theory, by scaling the dimensions (and consequently the electrical characteristics) of a transistor with a factor S, the transistor count increases by a factor S^2 (Moore's law) and the transistor switching frequency increases by a factor S, while keeping chip area and chip energy usage the same. Hence, the computational capabilities of chips increase by a factor S^3 per process generation. To maintain the same power usage, the transistor energy efficiency also has to improve with a factor S^3. This is achieved by scaling the transistor capacitance, which improves energy efficiency by a factor S, and by scaling the threshold and operating voltages, which provides another factor S^2 improvement in energy efficiency. However, Dennard's scaling no longer holds for process generations below 90 nm, since further scaling of the threshold voltage causes unacceptable levels of current leakage, and therefore the operating voltage has to remain roughly constant. Instead of improving the energy efficiency by S^3, in post-Dennard scaling the energy efficiency can only be improved by S. Hence, with each process generation we face a shortfall of S^2. While transistor count continues to increase according to Moore's law, the per-transistor speed and energy efficiency improvements slow down exponentially [23,24]. To deal with this, more and more portions of chips are not used all the time, or not at full frequency (which is referred to as 'dark silicon') [25]. This caused a shift to multicore design in 2005. Some applications can benefit from specialized, heterogeneous cores

that can be dynamically powered up for a given workload as in servers [26], or energy-efficient cores for computationally intensive applications [23]. However, this is not the case for bitcoin mining ASICs that continuously operate at peak performance, which results in extremely high and sustained power consumption [27]. Since 2005 also the search has initiated for new types of switches that improve performance and energy efficiency. It is unlikely that a new switch faster than CMOS transistors and consuming less power will be introduced into manufacturing on short term. Carbon nanotubes are promising, but it still will require several years until this reaches the manufacturing stage. 3D power scaling technology allows the continuation of Moore's law for the next 10–15 years via power-efficient vertical transistors. Eventually, switches will reach a fundamental performance limit, and any further improvement in computing performance can solely come from innovatives in system design [22]. The SHA-256 algorithm used for computing the block hashes in bitcoin mining however does not lend itself to significant micro-architectural design modifications. The only improvement for bitcoin mining ASICs is to migrate to the latest process technologies and possibly apply custom library cells or even custom physical layout [27]. Hence, the future improvement in performance and energy efficiency of bitcoin mining ASICs is expected to slow down.

Energy costs of bitcoin mining

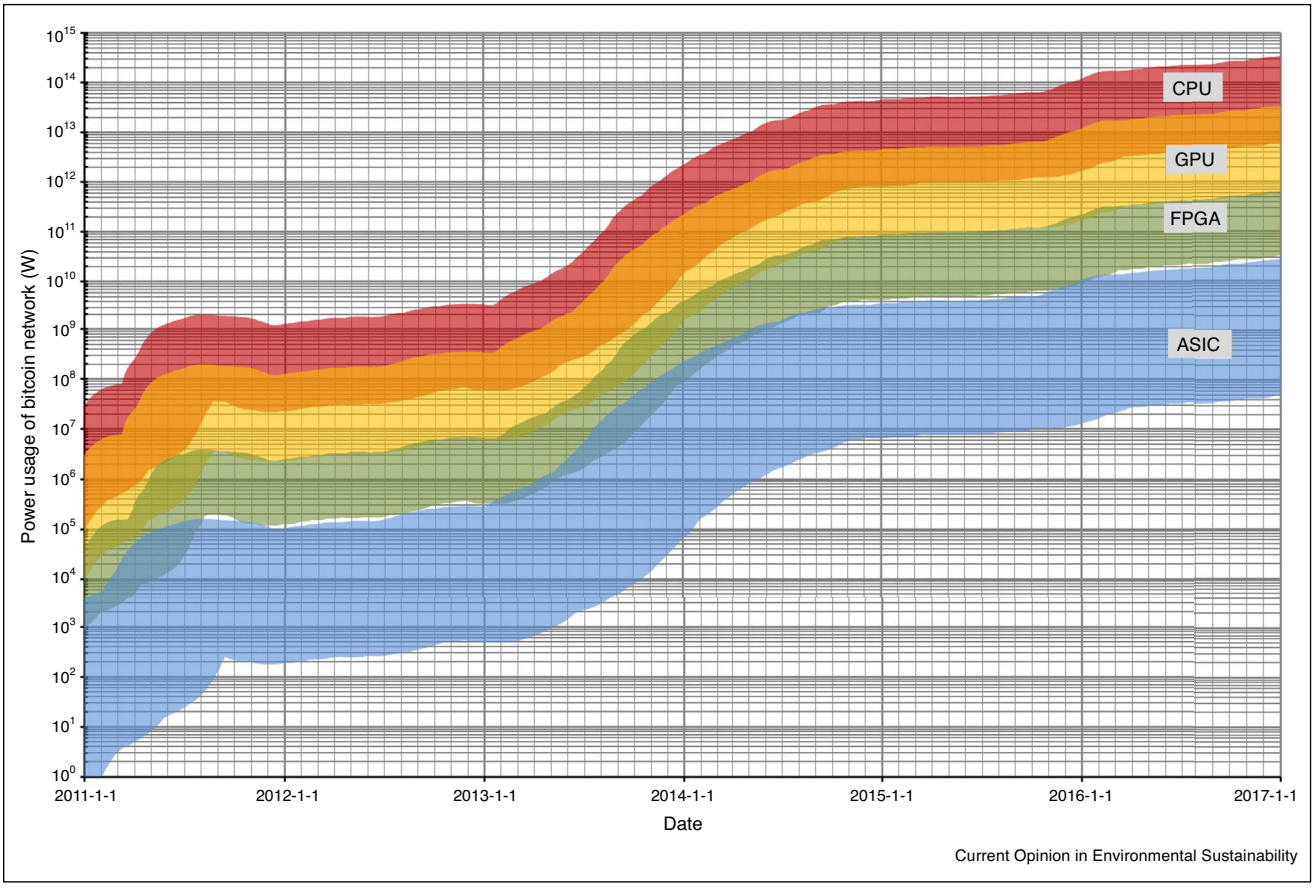
Next to the capital expenditure for bitcoin mining hardware, the main costs for bitcoin mining are the operational costs for running the hardware, which are mainly energy costs. There has been lot of debate on the total energy consumption of bitcoin mining, not only on Internet fora but also in scientific literature [10••,11••,20]. The estimates vary considerably, ranging from an energy consumption that is equivalent to the electricity generated by a small power plant (in the order of 10 MW) up to the electricity consumption of small to medium-sized countries such as Denmark, Ireland or Bangladesh (in the range of 3–6 GW).

O'Dwyer and Malone analyzed the energy footprint of bitcoin mining in 2014 [10••]. Their analysis is based on the observation that the power consumption of the bitcoin network (P, measured in W) can be computed from the hash rate of the bitcoin network (R, measured in h/s) and the energy efficiency of the bitcoin mining hardware (E, measured in h/J): $P = R/E$.

During the mining process, the miner computes the hash of a block of transactions. A block also contains other data, such as the hash of the latest accepted block in the blockchain, and a 'nonce' value that the miner can choose randomly. The aim of the miner is to find a nonce value such that the hash of the block is smaller than a target value T. In the bitcoin network, the 256-bits cryptographic hash of a block B is computed by applying the SHA-256 hash function [28] twice, $h(B) = \text{SHA256}(\text{SHA256}(B))$, which yields a hash that behaves approximately as a uniformly random value between 0 and $2^{256} - 1$. Hence, the only way to find a valid hash is to randomly try nonce values. This scheme is called 'proof-of-work'. The bitcoin network controls the difficulty for finding a valid hash by adjusting the target T every 2016 blocks, with the aim of keeping the average time to mine a new block near 10 min. The target is expressed in terms of the difficulty D by $D = T_{max}/T$, where T_{max} is the largest possible value of the target (which is $(2^{16} - 1)\,2^{208} \approx 2^{224}$). The probability that a nonce value yields a valid hash therefore is $p = T/2^{256} = T_{max}/(2^{256}D) \approx 1/(2^{32}D)$. The number of trials for choosing a nonce value that yields a valid hash is approximately geometrically distributed (assuming that these trials are independent, which of course does not hold for a single miner, but considers that multiple miners are independently performing the computations simultaneously). At rate R the expected time to find a valid nonce value therefore is $1/(pR) = 2^{32}D/R$, which equals 600 s. The hash rate of the bitcoin network then is $R \approx 2^{32}D/600$. Combining this with the energy efficiency E, the estimated power consumption of the bitcoin network is $P = R/E \approx 2^{32}D/(600E)$ [10••].

Figure 2 shows the power consumption (orders of magnitude) for various bitcoin mining hardware. Obviously, for any given date the estimated power consumption is realistic only when considering the hardware available at that time (see Table 1). The figure indicates that in January 2017 the actual power consumption could vary from 45 MW (using state-of-the art ASICs with 5×10^{10} h/J energy efficiency) up to 450 TW (using early generations of CPUs with 5×10^{3} h/J energy efficiency). Since the worldwide annual electricity consumption is about 2.3 TW, it is clear that 450 TW is completely unrealistic. A more realistic upper bound on the energy consumed can be derived when assuming that the revenue of bitcoin mining (see Figure 1) would be totally spent on energy costs (hence ignoring capital expenditure). The daily revenue of bitcoin mining, including block rewards and transaction fees, on January 1, 2017 was 1 961 203 USD (according to www.blockchain.info). This is a plausible number when considering that one block is mined every 10 min, which yields a daily revenue of 1 800 000 USD (at a block reward of 12.5 BTC and an exchange rate of 1000 USD) not considering transaction fees. With this revenue, the upper bound on the energy consumption is in the range of 400 MW (electricity price of 200 USD/MWh) up to 2.3 GW (electricity price of 35 USD/MWh). When taking 60 USD/MWh as an average case for electricity price, the energy consumption is 1.3 GW. The corresponding energy efficiency then is 1.8×10^{9} h/J,

Figure 2



Estimated power usage of bitcoin network ($2^{32}D/(600E)$) for various hardware (energy efficiency ranges (orders of magnitude) according to Table 1 (data sources: www.blockchain.info for historical data on difficulty; en.bitcoin.it/wiki/mining_hardware_comparison for energy efficiency of hardware).

and hence it is clear that bitcoin mining currently is only profitable when applying ASICs.

An even more accurate estimation of the energy consumption is derived when also considering the capital expenditure. Magaki *et al.* explored the design of purpose-built data centers running servers with large arrays of ASICs ('ASIC clouds') dedicated to bitcoin mining [20]. They consider three designs in which either energy, costs or total cost of ownership (TCO) are optimized, at an electricity price of 60 USD/MWh. In these three cases, the electricity costs are 7.5%, 16.9%, and 13.7% of the TCO. In the break-even case, where revenue equals TCO, the energy consumption is 100, 230 and 190 MW. The corresponding energy efficiency then is in the range of 1.1×10^{10} to 2.4×10^{10} h/J.

The ASICs that are currently being used by bitcoin miners, are most likely a mix of the newest available and some older ASICs. The actual mix used in practice is unknown. Bitcoin miners will not switch to newer hardware as long as mining with their current hardware is still profitable and the break-even point has not been reached yet at which revenues have covered the capital and operational expenditure of their current hardware. The future trend may well be to apply massive amounts of ASICs from older process technologies running at low power [27]. Bitcoin mining is very competitive. Bitcoins will be mined by those who can do it most cheaply, and others will be put out of business. It is therefore likely that surviving miners run the latest hardware at locations offering the lowest electricity costs to be competitive and to maximize profit.

Estimates published in scientific literature vary considerably:

- O'Dwyer and Malone estimated that the total power consumption for bitcoin mining would be around 100 MW to 10 GW [10••]. Without further substantiation, they conclude that an average of 3 GW would be most plausible (which is comparable to the Irish

national energy consumption). Our analysis however shows that is overestimated.

- McCook argues that chip-fabricator miners, who apply the ASICs that they design and manufacture themselves for mining, can mine for up to 30% cheaper than retail miners, and that they form the vast majority of the hash power [11••]. Applying the 80-20 rule, assuming chip fabricators hold 80% and retail miners hold 20% of the hash power, the energy efficiency on average is estimated at 2.5 Gh/J, which corresponds to a power consumption of 120 MW.
- Magaki *et al.* state that the global power budget dedicated to ASIC clouds is estimated by experts to be in the range of 300–500 MW [20].

We conclude that although the energy consumption could be as low as 45 MW when solely using the latest bitcoin mining ASICs, in practice the energy consumption most likely is in the range of 100–500 MW (which corresponds to 3–16 PJ per year). Hence, the order of magnitude of the energy consumption is 100 MW.

To put things into perspective, McCook also compares the sustainability of bitcoin mining with the sustainability of gold mining and the banking system [11••]. The energy used per year for gold mining and recycling is estimated at 500 PJ, for printing paper banknotes and minting coins at 40 PJ, and for the banking system, considering ATMs and bank branches (which of course provide more services than just handling transactions), at 2340 PJ. Compared to these numbers, the energy used for bitcoin mining in the range of 3–16 PJ is relatively small. Still, the proportion of bitcoin in the current financial system is relatively small, and when bitcoin scales up, so will the effort for bitcoin mining.

Another line of thought to deal with the criticism that proof-of-work as applied in bitcoin wastes energy, is to replace the computation of hashes by more 'meaningful' tasks. This has been applied in other electronic currencies. For instance, NooShare proposes the scheduling of arbitrary Monte-Carlo simulations as a proof-of-work, Primecoin proposes the computation of long chains of prime numbers (Cunningham chains), and Permacoin proposes proofs of retrievability [7•].

There are also other factors that impact the sustainability of bitcoin [29]. For instance, bitcoin is not suited for real-time transactions due to the delay between the injection of a transaction into the bitcoin network and the inclusion of the transaction in a mined block that is added to the blockchain, and for the transaction actually to be confirmed a sufficient amount of subsequent blocks has to be added to the blockchain [30,31]. Other concerns are the growing size of the blockchain, and security [32–34,7•].

Alternatives for proof-of-work

Various alternative consensus mechanisms have been proposed to address the energy consumption of proof-of-work [35]. In proof-of-stake, users are required to prove the ownership of their amount of coins. Users create ' coinstake' transactions in which they send the coins in their possession to themselves and add a predefined percentage as reward. In the mining process, still the hash of a block has to be computed that is smaller than a target value. A block however does not include a nonce value that can be modified by the miner, but a time-stamp that changes every second. Hence, miners cannot rely on computational power, but they can only compute one hash every second. The miner that wins the block, receives the transaction reward. The difficulty is determined individually for every user: it is inversely proportional to the coin age, which is the amount of coins times the time period that the user held these coins. Hence, users with a large coin age have a higher chance to mine a block. When a block is mined that includes a coinstake transaction, the coin age of the winner is reset. Hence, proof-of-stake is a raffle-like scheme, with repeatedly occurring new chances for all participants [36–38]. Also a combination of proof-of-work and proof-of-stake has been proposed, in which a fraction of the proof-of-work block reward is raffled among all active nodes, while their stake determines the amount of raffle tickets [39].

Another alternative is proof-of-space, where the miner must employ a specified amount of memory to compute the proof [40,41]. In proof-of-space-time, the miner must prove that he stored data over a period of time [42].

Although these alternatives largely reduce the energy consumption as with proof-of-work, there still are security issues when applying them to public blockchains [39,38].

Blockchains

Blockchain is at the basis of currencies such as bitcoin, but it can also be used in many other financial and commercial applications [43–49,35]. A prominent example is smart contracts, for instance as offered in Ethereum [50]. A contract can execute a transfer when certain events happen, such as payment of a security deposit, while the correct execution is enforced by the consensus protocol [51,52].

Blockchains can be classified as public blockchains, private blockchains or consortium blockchains [35]. Bitcoin is an example of a public blockchain, in which all records are visible to the public and everyone can take part in the consensus process. A private blockchain is fully controlled by one organization, with a closed group of known participants, which implies a centralized rather than a decentralized network. A consortium blockchain is partially decentralized, where transactions are validated by a selected set of nodes. Private and consortium blockchains

may permission other users to read records in the blockchain. Public blockchains rely on a consensus protocol such as proof-of-work, which ensures that transactions cannot be tampered as long an no single miner controls more than 50% of the network's hash power. Transactions in private or consortium blockchains are editable as long as the major participants have reached an agreement, and hence a strong consensus protocol such as proof-of-work is not required. This reduces security, but improves efficiency and latency, and hence energy consumption is barely an issue.

Conclusion

In this review we described the basic operation of bitcoin mining and we explored the developments in the hardware used for bitcoin mining. The proof-of-work scheme is compute-intensive and hence energy demanding, but essential for dealing with the double-spending problem and security of the blockchain. The mining hardware has evolved from CPUs, GPUs and FPGAs to ASICs, with an exponential increase in performance and energy efficiency. It is expected however that this trend will slow down in the next decade. We discussed the energy footprint of bitcoin mining, which has been subject of debate. Our estimates show that the order of magnitude for the energy consumption is 100 MW. As bitcoin becomes more popular, the effort for bitcoin mining will increase. Since bitcoin mining is very competitive, only those miners will survive who apply the most competitive mining hardware and benefit from the lowest electricity costs. The sustainability of bitcoin on itself therefore is not primarily at risk due to energy consumption. We also briefly reviewed alternative schemes such as proof-of-stake, which are far less energy demanding. Finally, we looked at other applications of blockchain technology, which are currently receiving lots of interest. Private and consortium blockchains are only partially decentralized, which relaxes the need and effort for proof-of-work schemes, and hence energy consumption may be barely an issue.

Acknowledgements

We kindly thank the anonymous reviewers for their valuable comments.

References and recommended reading

Papers of particular interest, published within the period of review, have been highlighted as:

- • of special interest
- •• of outstanding interest

1. Ali R, Barrdear J, Clews R, Southgate J: **The economics of digital currencies**. *Bank Engl Q Bull* 2014, **2014**:276-286.

2. Mikołajewicz-Woźniak A, Scheibe A: **Virtual currency schemes — the future of financial services**. *Foresight* 2015, **17**:365-377 http://dx.doi.org/10.1108/FS-04-2014-0021.

3. Beer C, Weber B: **Bitcoin — the promise and limits of private innovation in monetary and payment systems**. *Monet Policy Econ* 2014, **4**:53-66.

4. Nakamoto S: *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008.

5. Zohar A: **Bitcoin: under the hood**. *Commun ACM* 2015, **58**:104-113 http://dx.doi.org/10.1145/2701411.

6. • Antonopoulos AM: *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media; 2014. ISBN: 978-1-4493-7404-4. http://chimera.labs.oreilly.com/books/1234000001802/index.html.
This book outlines the technical operation of bitcoin.

7. • Tschorsch F, Scheuermann B: **Bitcoin and beyond: a technical survey on decentralized digital currencies**. *IEEE Commun Surv Tutor* 2016, **18**:2084-2123 http://dx.doi.org/10.1109/COMST.2016.2535718.
This survey describes the basics of bitcoin, and discusses security threats and privacy properties, as well as the proof-of-work scheme and alternative approaches.

8. Garay J, Kiayias A, Leonardos N: **The bitcoin backbone protocol: analysis and applications**. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer; 2015:281-310.

9. • Chuen DLK (Ed): *Handbook of Digital Currency*. Academic Press; 2015. ISBN: 978-0-12-802117-0.
This book covers technical, economical and financial aspects of bitcoin.

10. •• O'Dwyer KJ, Malone D: **Bitcoin mining and its energy footprint**. *Irish Signals & Systems Conference 2014 and 2014 China–Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*. IET; 2014:280-285.
In this paper the energy footprint of the bitcoin network is computed. It is estimated that the electricity consumption of bitcoin mining is on par with that of Ireland.

11. •• McCook H: *An Order-of-Magnitude Estimate of the Relative Sustainability of the Bitcoin Network*. 2015 In: *https://www.academia.edu/7666373/An_Order-of-Magnitude_Estimate_of_the_Relative_Sustainability_of_the_Bitcoin_Network_-_3rd_Edition*.
This paper compares the sustainability of the bitcoin network with the banking industry, the gold production industry, and the process of printing and minting of physical currency.

12. Harwick C: **Cryptocurrency and the problem of intermediation**. *Independ Rev* 2016, **20**:569-588.

13. Grant G, Hogan R: **Bitcoin: risks and controls**. *J Corp Account Finance* 2015, **26**:29-35 http://dx.doi.org/10.1002/jcaf.22060.

14. Walch A: **The bitcoin blockchain as financial market infrastructure: a consideration of operational risk**. *N Y Univ J Legisl Public Policy* 2015, **18**:837-893.

15. Angel JJ, McCabe D: **The ethics of payments: paper, plastic, or bitcoin?** *J Business Ethics* 2015, **132**:603-611.

16. Back A: *Hashcash — A Denial of Service Counter-Measure*. 2002 In: *ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf*.

17. Hayes AS: **Cryptocurrency value formation: an empirical study leading to a cost of production model for valuing bitcoin**. *Telemat Informat* 2016 http://dx.doi.org/10.1016/j.tele.2016.05.005. (in press).

18. Kaskaloglu K: **Near zero bitcoin transaction fees cannot last forever**. *The International Conference on Digital Security and Forensics (DigitalSec2014)*; *The Society of Digital Information and Wireless Communication: 2014:91-99*.

19. •• Taylor MB: **Bitcoin and the age of bespoke silicon**. In *Proceedings of the 2013 International Conference on Compilers, Architectures and Synthesis for Embedded Systems, CASES'13*. Piscataway, NJ, USA: IEEE Press; 2013. pp. 16:1–16:10. ISBN: 978-1-4799-1400-5. http://dl.acm.org/citation.cfm?id=2555729.2555745.
This paper describes the history of bitcoin mining hardware, especially the development of ASICs, as well as the incentives and strategies of bitcoin miners.

20. Magaki I, Khazraee M, Gutierrez LV, Taylor MB: **ASIC clouds: specializing the datacenter**. In *Proceedings of the 43rd International Symposium on Computer Architecture, ISCA'16*.

Piscataway, NJ, USA: IEEE Press; 2016, 178-190 http://dx.doi.org/10.1109/ISCA.2016.25:. ISBN: 978-1-4673-8947-1.

21. Wang L, Liu Y: **Exploring miner evolution in bitcoin network**. In *Proceedings 16th International Conference on Passive and Active Network Measurement; vol 8995 of Lecture Notes in Computer Science Series*. Springer; 2015:290-302 http://dx.doi.org/10.1007/978-3-319-15509-8_22.

22. Gargini PA: **How to successfully overcome inflection points, or long live Moore's law**. *Comput Sci Eng* 2017, **19**:51-62 http://dx.doi.org/10.1109/MCSE.2017.32.

23. Venkatesh G, Sampson J, Goulding N, Garcia S, Bryksin V, Lugo-Martinez J, Swanson S, Taylor MB: **Conservation cores: reducing the energy of mature computations**. In *Proceedings of the Fifteenth Edition of ASPLOS on Architectural Support for Programming Languages and Operating Systems*. ACM; 2010 http://dx.doi.org/10.1145/1736020.1736044. ISBN: 978-1-60558-839-1; 205-218.

24. Esmaeilzadeh H, Blem E, Amant RS, Sankaralingam K, Burger D: **Power challenges may end the multicore era**. *Commun ACM* 2013, **56**:93-102 http://dx.doi.org/10.1145/2408776.2408797.

25. Taylor MB: **A landscape of the new dark silicon design regime**. *IEEE Micro* 2013, **33**:8-19.

26. Hardavellas N, Ferdman M, Falsafi B, Ailamaki A: **Toward dark silicon in servers**. *IEEE Micro* 2011, **31**:6-15.

27. Barkatullah J, Hanke T: **Goldstrike 1: Cointerra's first-generation cryptocurrency mining processor for bitcoin**. *IEEE Micro* 2015, **35**:68-76.

28. NIST: *FIPS PUB 180-4, Secure Hash Standard (SHS)*. 2015 http://dx.doi.org/10.6028/NIST.FIPS.180-4.

29. Extance A: **Bitcoin and beyond**. *Nature* 2015, **526**:21-23.

30. Decker C, Seidel J, Wattenhofer R: **Bitcoin meets strong consistency**. In *Proceedings of the 17th International Conference on Distributed Computing and Networking, ICDCN'16*. New York, NY, USA: ACM; 2016 http://dx.doi.org/10.1145/2833312.2833321. 13:1–13:10. ISBN: 978-1-4503-4032-8.

31. Karame GO, Androulaki E, Roeschlin M, Gervais A, Čapkun S: **Misbehavior in bitcoin: a study of double-spending and accountability**. *ACM Trans Inform Syst Security* 2015, **18**:1-32 http://dx.doi.org/10.1145/2732196.

32. Gervais A, Ritzdorf H, Karame GO, Capkun S: **Tampering with the delivery of blocks and transactions in bitcoin**. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS'15*. New York, NY, USA: ACM; 2015, 692-705 http://dx.doi.org/10.1145/2810103.2813655:. ISBN: 978-1-4503-3832-5.

33. Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S: **On the security and performance of proof of work blockchains**. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS'16*. New York, NY, USA: ACM; 2016, 3-16 http://dx.doi.org/10.1145/2976749.2978341:. ISBN: 978-1-4503-4139-4.

34. Paul G, Sarkar P, Mukherjee S: **Towards a more democratic mining in bitcoins**. In In *Proceedings of 10th International Conference on Information Systems Security (ICISS); vol 8880 of Lecture Notes in Computer Science (LNCS).* Edited by Prakash A, Shyamasundar R. *Proceedings of 10th International Conference on Information Systems Security (ICISS); vol 8880 of Lecture Notes in Computer Science (LNCS)* Cham: Springer International Publishing; 2014:185-203 http://dx.doi.org/10.1007/978-3-319-13841-1_11. ISBN: 978-3-319-13841-1.

35. Zheng Z, Xie S, Dai H, Chen X, Wang H: **An overview of blockchain technology: architecture, consensus, and future trends**. *Proceedings of 6th IEEE International Congress on Big Data* 2017.

36. King S, Nadal S: *PPcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. 2012.

37. Bentov I, Gabizon A, Mizrahi A: *Cryptocurrencies Without Proof of Work*. 2014arXiv:1406.5694.

38. Kiayias A, Konstantinou I, Russell A, David B, Oliynykov R: *A Provably Secure Proof-of-Stake Blockchain Protocol. Cryptology ePrint Archive, Report 2016/889*. 2016 In: *http://eprint.iacr.org/2016/889*.

39. Bentov I, Lee C, Mizrahi A, Rosenfeld M: *Proof of Activity: Extending Bitcoin's Proof of Work Via Proof of Stake. Cryptology ePrint Archive, Report 2014/452*. 2014 In: *http://eprint.iacr.org/2014/452*.

40. Ateniese G, Bonacina I, Faonio A, Galesi N: **Proofs of space: when space is of the essence**. *International Conference on Security and Cryptography for Networks*. Springer; 2014:538-557.

41. Dziembowski S, Faust S, Kolmogorov V, Pietrzak K: **Proofs of space**. *Advances in Cryptology — CRYPTO 2015; vol 9216 of Lecture Notes in Computer Science Series*. Springer; 2015:585-605 http://dx.doi.org/10.1007/978-3-662-48000-7_29.

42. Moran T, Orlov I: *Proofs of Space–Time and Rational Proofs of Storage. Cryptology ePrint Archive, Report 2016/045*. 2016 . Report 2016/035 In: *https://eprint.iacr.org/2016/035*.

43. Underwood S: **Blockchain beyond bitcoin**. *Commun ACM* 2016, **59**:15-17 http://dx.doi.org/10.1145/2994581.

44. Umeh J: **Blockchain double bubble or double trouble?** *ITNOW* 2016, **58**:58-61.

45. Fanning K, Centers DP: **Blockchain and its coming impact on financial services**. *J Corp Account Finance* 2016, **27**:53-57 http://dx.doi.org/10.1002/jcaf.22179.

46. Yli-Huumo J, Ko D, Choi S, Park S, Smolander K: **Where is current research on blockchain technology? A systematic review**. *PLOS ONE* 2016, **11** http://dx.doi.org/10.1371/journal.pone.0163477.

47. BitFury Group, Garzik J: *Public Versus Private Blockchains — Part 1: Permissioned Blockchains. White Paper*. 2015 In: *http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf*.

48. BitFury Group, Garzik J: *Public Versus Private Blockchains — Part 2: Permissionless Blockchains. White Paper*. 2015 In: *http://bitfury.com/content/5-white-papers-research/public-vs-private-pt2-1.pdf*.

49. Forte P, Romano D, Schmid G: *Beyond Bitcoin — Part I: A Critical Look at Blockchain-Based Systems. Cryptology ePrint Archive, Report 2015/1164*. 2015 In: *http://eprint.iacr.org/2015/1164*.

50. Wood G: *Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper*. 2014:151 In: *http://gavwood.com/paper.pdf*.

51. Luu L, Chu DH, Olickel H, Saxena P, Hobor A: **Making smart contracts smarter**. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS'16*. New York, NY, USA: ACM; 2016, 254-269 http://dx.doi.org/10.1145/2976749.2978309:. ISBN: 978-1-4503-4139-4.

52. Luu L, Teutsch J, Kulkarni R, Saxena P: **Demystifying incentives in the consensus computer**. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS'15*. New York, NY, USA: ACM; 2015, 706-719 http://dx.doi.org/10.1145/2810103.2813659:. ISBN: 978-1-4503-3832-5.