Bus Inf Syst Eng 62(6):599–608 (2020)
https://doi.org/10.1007/s12599-020-00656-x

CATCHWORD

The Energy Consumption of Blockchain Technology: Beyond Myth

Johannes Sedlmeir · Hans Ulrich Buhl · Gilbert Fridgen · Robert Keller

Received: 10 February 2020 / Accepted: 9 May 2020 / Published online: 19 June 2020

Abstract When talking about blockchain technology in academia, business, and society, frequently generalizations are still heared about its – supposedly inherent – enormous energy consumption. This perception inevitably raises concerns about the further adoption of blockchain technology, a fact that inhibits rapid uptake of what is widely considered to be a groundbreaking and disruptive innovation. However, blockchain technology is far from homogeneous, meaning that blanket statements about its energy consumption should be reviewed with care. The article is meant to bring clarity to the topic in a holistic fashion, looking beyond claims regarding the energy consumption of Bitcoin, which have, so far, dominated the discussion.

Accepted after two revisions by Ulrich Frank.

J. Sedlmeir · H. U. Buhl · G. Fridgen · R. Keller
Project Group Business and Information Systems Engineering of the Fraunhofer FIT, Bayreuth, Germany
e-mail: hans-ulrich.buhl@fim-rc.de

G. Fridgen
e-mail: gilbert.fridgen@uni.lu

R. Keller
e-mail: robert.keller@fim-rc.de

J. Sedlmeir (✉)
FIM Research Center, University of Bayreuth, Bayreuth, Germany
e-mail: johannes.sedlmeir@fit.fraunhofer.de

H. U. Buhl · R. Keller
FIM Research Center, University of Augsburg, Augsburg, Germany

G. Fridgen
SnT - Interdisciplinary Center for Security, Reliability and Trust, University of Luxembourg, Luxembourg, Luxembourg

Keywords Blockchain · Cryptocurrency · Energy consumption · Distributed ledger technology · Sustainability

1 Introduction

Blockchain technology entered public awareness with its first application, the cryptocurrency Bitcoin (Nakamoto 2008), which was established in 2009 and currently exhibits a market capitalization of more than 100 billion USD. In the last decade, blockchain technology has developed significantly and is now implemented in a wide range of scenarios, including Ethereum or Hyperledger Fabric, which allow distributed platforms to function with unprecedented versatility (Lockl et al. 2020). Consequently, many researchers and practitioners have realized that blockchain technology holds disruptive potential beyond its use in cryptocurrencies (Beck 2018; Fridgen et al. 2018a; Labazova et al. 2019). Generally speaking, blockchain technology permits secure transactions to be made without the involvement of intermediaries, and is, therefore, appealing to individuals as well as to industry and the public sector. However, Bitcoin still dominates many people's perceptions of blockchain technology. Moreover, it is well-known that Bitcoin consumes an enormous amount of energy (De Vries 2018). (Strictly speaking, we cannot consume energy, but merely change its form from valuable (e.g., electricity) to less valuable (e.g., heat) energy. Nevertheless, we will stick to the common usage of the phrase here.) Consequently, one frequently encounters claims that the energy consumption of blockchain technology in general is problematic (Truby 2018). Considering the current discussions regarding climate change and sustainability, these statements could

therefore inhibit or delay the widespread adoption of blockchain technology (Beck et al. 2018).

This article challenges the common prejudices regarding the energy consumption of the supposedly homogeneous blockchain technology by providing a detailed analysis of current scientific knowledge. It, thereby, addresses the energy consumption of IS, in general a subject for which BISE traditionally takes responsibility (Buhl and Jetter 2009; Schmidt et al. 2009). In particular, it also addresses the need for a detailed investigation into the energy consumption of blockchain technology, as pointed out in Beck et al. (2017). In Sect. 2, we first provide some technical background for Proof-of-Work (PoW) blockchains and determine the level of their energy consumption. Using these estimates, we illustrate that today's PoW cryptocurrencies do, indeed, consume an amount of energy which may be regarded as disproportionate when compared to the currencies' actual utility. However, we also argue that the energy consumption associated with a widespread uptake of PoW cryptocurrencies is not likely to become a major threat to the climate in the future. In Sect. 3, we put these results into perspective by presenting blockchains with alternative consensus mechanisms. We illustrate that these kinds of blockchain technology already consume several orders of magnitude less energy than the first generation PoW blockchains and that these blockchains, thus, largely mitigate the energy problem. However, we argue that, in addition to consensus, the redundancy underlying all types of blockchain technology can make blockchain-based IT solutions considerably more energy-intensive than a non-blockchain, centralized alternative. In Sect. 4, we discuss this issue and also give an overview of methods and concepts which could further decrease the energy consumption of blockchain technology. In Sect. 5, we illustrate our findings by a first rough comparison of the energy consumption of some non-blockchain, centralized systems to that of basic blockchain architectures. We conclude with with an outlook and suggested topics for further research in Sect. 6.

2 Proof-of-Work Blockchains

2.1 Technological Basics

Bitcoin, the first application built on blockchain technology, is a decentralized payment system in which all participating computers ("nodes") store a copy – or, more precisely, a replica, since there is no distinguished master – of the associated ledger. A ledger is commonly defined as a collection of accounts, stating one's current rights of ownership of a particular asset – in the case of Bitcoin, units of the eponymous cryptocurrency. The underlying technology, blockchain, provides a means to store information chronologically and redundantly on a decentralized database, and an agreement process through which the nodes synchronize and modify their global state ("operate transactions") (Crosby et al. 2016). It is, therefore, not exclusively suitable for use with cryptocurrencies, but can be applied to many processes in which the involvement of an intermediary such as a bank, a notary, or any (digital) platform owner is not desirable.

Blockchains, in general, achieve this synchronization by linking transactions to form batches ("blocks") and adding these, sequentially, to the existing linear data structure ("chain"). Utilizing Merkle trees and hash-pointers, this data structure is highly tamper-sensitive, making retrospective manipulations easy to detect. Agreement about which new blocks to append is reached using a so-called consensus mechanism. Anyone can run a node for the common cryptocurrencies and participate in the consensus mechanism of their underlying blockchains using public key cryptography and hence without any form of registration. Consequently, blockchains underlying such open systems, which allow for unrestricted access and participation, are termed *permissionless*. Since, on a permissionless blockchain, the inclusion of a distinct entity to provide accounts and passwords is not viable, authentication based on a public key infrastructure is highly suitable. For such blockchains, a simple voting-based agreement process based on "one man – one vote" is not secure, since a potential attacker could simply create multiple accounts to gain a majority and take control of the system; this is called a Sybil attack (Douceur 2002).

Bitcoin's key innovation was to provide a suitable consensus mechanism for the use in this scenario. Specifically, Bitcoin combined several well-known concepts from cryptography to form the so-called PoW. This refers to the right to create a new block from a subset of queued transactions when one finds a solution to a cryptographic, computationally intensive puzzle. The process of searching for a solution is called "mining". This results in coupling the voting weight to a scarce resource – computing power and thus energy – and hence prevents Sybil attacks. The mining process is economically incentivized in that participants are rewarded for every valid block that is found and disseminated. The reward typically consists of a certain amount of the associated cryptocurrency and the fees for the associated transactions. The value of the former is proportional to the cryptocurrency's market price, so the success of cryptocurrencies on financial markets in the last years has provided a very strong incentive to participate in mining. In turn, this has led to an enormous energy consumption associated with the underlying PoW blockchains.

It is essential to note that the high energy consumption of PoW blockchains is neither the result of inefficient algorithms nor of outdated hardware. Strikingly, such blockchains are "energy-intensive by design". It is their high energy consumption that protects PoW blockchains from attacks: Depending on the scenario, an attacker must bear at least 25 to 50% of the total computing power that participating miners use for mining – and, thus, the same proportion of the total energy consumption (under the assumption of equal hardware) – to be able to successfully manipulate or control the system (Eyal and Sirer 2014). Consequently, the more valuable a PoW cryptocurrency is, the better it is protected against attacks, confirming that PoW is, indeed, a thoughtful design.

2.2 General Estimates

Starting with the work of O'Dwyer and Malone (2014), researchers have analyzed the energy consumption caused by Bitcoin in numerous scientific publications over recent years (Stoll et al. 2019). However, results regarding the energy consumption of PoW cryptocurrencies and blockchain technology in general are rare. Determining the exact value for the energy consumption of a multitude of open, distributed networks is a hard task because the precise number of participants, the properties of their hardware, and the effort which they put into mining are unknown. Fortunately, however, one can obtain good estimates for a lower and an upper bound of the energy consumption of any PoW blockchain by following Vranken (2017) and Krause and Tolaymat (2018): Since both the difficulty of the cryptographic puzzles and the frequency at which solutions are found are easily observable, one can calculate the expected value of the minimum frequency of calculations ("hash-rate") needed to solve the puzzles as often as observed. This gives a lower bound of the energy consumption of an arbitrary PoW blockchain:

$$\begin{aligned}\text{total power consumption} &\geq \text{total hash rate} \\ &\times \text{min energy per hash.}\end{aligned} \tag{1}$$

This estimate indicates the lower bound, reflecting the likelihood that more solutions are found than disseminated, that further computations – in addition to mining – are being carried out, and that not every miner has the most energy-efficient hardware.

Both the current hash rate of a public blockchain and the energy efficiency of the most efficient mining hardware can easily be retrieved from online material. However, one must be aware that mining hardware is in general blockchain-dependent because the algorithms used for hashing can differ. For example, Bitcoin uses SHA256, for which very efficient application-specific integrated circuits (ASICS) exist, i.e., chips that are highly optimized for computing hash values and, thus, for solving the puzzles. On the other hand, Ethereum was designed to prevent the use of highly specific mining hardware, so general-purpose GPUs can be used for mining. Note that (1) does not depend on any other parameters and, therefore, gives a very reliable lower bound. Entering the current numbers – retrieved from Coinmarketcap (2020) and Coinswitch (2019) on 2020-02-05 – into (1) yields a lower bound for power consumption of 6.8 GW, which equates to an annual energy requirement of at least 60 TWh. Alternatively, one could, of course, also integrate the time-dependent lower bound over the period under consideration.

One can also determine an upper bound for the energy requirement of the mining process for a PoW blockchain, assuming honest and rational miners whose utility from mining is solely financial profit: Participation in the mining process is only profitable as long as the expected revenue from mining is higher than the associated costs:

$$\begin{aligned}\text{mining rewards} + \text{transaction fees} &= \text{tot. mining revenue} \\ &\geq \text{tot. mining costs} \\ &\geq \text{tot. energy consumption} \\ &\times \text{min.electricity price.}\end{aligned}$$

A few easy manipulations yield the desired upper bound:

$$\begin{aligned}&\text{total power consumption} \\ &\leq \frac{\text{block reward} \times \text{coin price} + \text{transaction fees}}{\text{avg. blocktime} \times \text{min. electricity price}}.\end{aligned} \tag{2}$$

As hardware costs represent a substantial part of the costs side, and electricity prices vary significantly around the globe, we cannot assume that the upper bound is very tight. The block reward, i.e., the number of cryptocurrency coins one receives for solving a puzzle, the price of a coin, and current transaction fees are, again, publicly observable for every PoW cryptocurrency, meaning that only sensitive number which has to be estimated is the minimum electricity price. De Vries (2018), for example, argues that $0.05\,\frac{\text{USD}}{\text{kWh}}$ is a reasonable lower bound for electricity prices. This gives an upper bound of approximately 125 TWh per year for the energy consumption of Bitcoin, using data from Coinmarketcap (2020) for 2020-02-05.

We repeated the calculation of the lower bound (1) and the upper bound (2) for the remaining 4 PoW cryptocurrencies with market capitalization of at least 1 billion USD. Figure 1 displays the resultant ranges for their respective energy consumption:

We see that the lower and upper bounds are, in general, quite close and, therefore, represent a meaningful estimate of the actual energy consumption for each of the 5 major PoW cryptocurrencies. A manifestation of this fact could

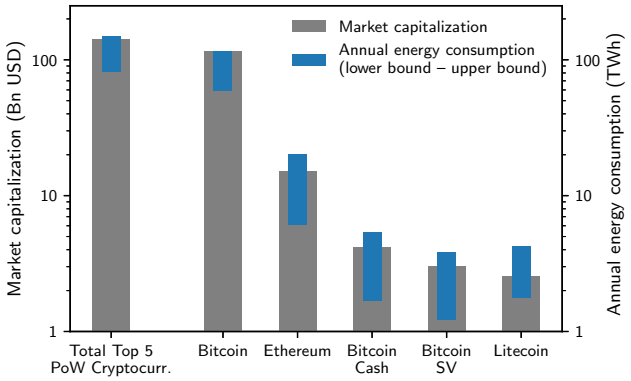

Fig. 1 Market capitalization and the computed bounds on energy consumption for the 5 highest valued Proof-of-Work cryptocurrencies. Note the logarithmic scale on the y-axis

be observed when in the course of a general drop in financial markets due to the Corona pandemic, market prices for Bitcoin dropped by up to 40% in March 2020. This implies a drop of the upper bound (2) in our model by the same rate, and, indeed, the total hash rate was observed to drop by approximately 30% shortly after: Seemingly, mining was no longer profitable for some miners at this point (Beincrypto 2020). This incident also illustrates that the upper bound is highly sensitive on the economic circumstances: Assuming that electricity prices dropped by the same rate as the prices for cryptocurrencies – which is in fact conceivable in an economic crisis – the upper bound (2) would remain unchanged. On the other hand, if electricity prices generally dropped by 50%, e.g., due to decreased demand or increased feed-in of renewables, or a rush for cryptocurrencies led to an increase of their prices by 100% and, therefore, to a level that we have already observed by the beginning of 2018, our upper bound would double in each of the scenarios, and even quadruple if both happened to occur at the same time. Consequently, we learn that we cannot take for granted that the given upper bound holds forever; it merely represents a snapshot for the current economic situation.

We also observe that the expected energy consumption of the 5 investigated cryptocurrencies strongly correlates with their market capitalization, which makes sense since parameters, such as block reward per time, are comparable among the cryptocurrencies and total transaction fees are generally low compared to block rewards. Moreover, the total market capitalization for all other PoW cryptocurrencies is significantly lower than that of Bitcoin itself. This indicates that the total energy consumption of *all* PoW cryptocurrencies other than Bitcoin will fall below our upper bound for the energy consumption of Bitcoin. A more precise estimate could be obtained by applying (2) to all remaining PoW cryptocurrencies. This would, however, be a tedious task, as one would have to collect specific parameters, such as block reward and average block time, for each PoW cryptocurrency, of which there are currently more than 1000.

In both estimates, we have, so far, only taken into account the energy consumption involved in mining, i.e., solving the cryptographic puzzles, and neglected the energy consumption of the other tasks which have to be performed on the participating nodes, mainly, validating new blocks and updating their local databases accordingly. This is, in fact, a reasonable approximation: for the lower bound, we only lose some tightness. To justify the validity of our upper bound, we argue that the energy consumption associated with maintaining the nodes, mining excluded, is, in fact, negligible compared to the energy consumption of mining for today's major PoW blockchains: To validate a single block in today's cryptocurrencies, every node must typically download up to a few Megabytes of data and perform as many as several thousand hash computations, as well as a comparable number of corresponding computations and database operations. For example, in a 1 MB block used in Bitcoin, there can only be a maximum of around 2000 transactions. These are the leaves of the Merkle tree and, therefore, give a total of 4000 hash value computations and a similar number of corresponding database manipulations and signature checks. By comparison, finding a single block currently involves around 10^{23} hash computations to solve a puzzle in Bitcoin, around 10^{20} hash computations for Bitcoin Cash and Bitcoin SV, and around 10^{15} hash computations for Ethereum and Litecoin. Even for a million nodes – and taking into account differences in efficiency between common and specialized mining hardware, given that ASICS can be millions of times more efficient than CPUs at computing hashes – the energy consumption associated with mining is still *orders of magnitude* higher than the energy consumption required to maintain the nodes (De Vries 2018).

At this point, it is important to emphasize that further increasing the energy efficiency of mining hardware would not reduce a PoW blockchain's energy requirements in the long term: To keep the average time for solving a puzzle constant, and, hence, to ensure the security and constant functionality of the network, the difficulty of the cryptographic puzzles is periodically adapted to the total computing power of the network. Since energy costs outweigh hardware costs in the long run, participants with improved hardware can solve more puzzles at the same energy costs. Other participants have to follow suit with the competition. This, in turn, involves higher overall computing power, and means that the difficulty of the puzzle needs to be increased so that it is, on average, solved as frequently as before. Hence, it is only in the (short-term) conversion phase that positive effects are conceivable. In fact, competition in the

mining hardware market, resulting from the hype around cryptocurrencies, has dramatically increased the energy efficiency of mining hardware in the last decade. In the long term, it is to be expected that even with groundbreaking innovation in the energy efficiency of mining hardware, Bitcoin's and other PoW blockchains' energy requirements will remain at the previous level unless the remaining economic quantities on the right-hand side of (2) change considerably.

2.3 Closing Notes on the Energy Consumption of PoW Blockchains

In summary, our lower and upper bounds represent different approaches and use different quantities that have to be estimated. Yet, these bounds are very consistent in the case of all of the cryptocurrencies we investigated. For example, we determined electricity consumption to be between 60 and 125 TWh per year for Bitcoin. This is in the range of the annual electricity consumption of countries such as Austria (75 GWh) and Norway (125 GWh). However, as cryptocurrencies currently process only few transactions per second, the theoretical limit is typically in the low two- or three-digit range, e.g., approx. 15 for Ethereum and Bitcoin and 100 for Bitcoin Cash. This is primarily determined by the parameters 'average block time', 'minimum size of transactions', and 'maximum block size' (Georgiadis 2019). Accordingly, a single transaction currently requires enough electrical energy to meet the needs of the average size German household for weeks, or even months. By contrast, traditional payment systems process, on average, thousands of transactions per second, and as many as tens of thousands at peak times. In their publication in "Nature Climate Change", Mora et al. (2018) extrapolate the energy consumption of a single Bitcoin transaction to the order of magnitude required for handling payments on a global scale. They claim that if Bitcoin were to handle the number of transactions required by a worldwide payment system, the associated emissions alone would lead to a global temperature increase of 2 °C in the coming decades. However – as has already been pointed out in a critical 'Matters Arising' response by Dittmar and Praktiknjo (2019) – when increasing the blocksize and, therefore, the throughput, according to our previous arguments, the energy consumption associated with mining would remain constant, and the energy consumption associated with the remaining tasks would still be negligible. This means that, overall, there would be no noticeable increase in total energy consumption. This argument is, however, based on the assumption that the economic quantities from the estimate of the upper bound (2), namely, the prices for electricity and the respective cryptocurrency, remain constant.

In practice, however, the blocks cannot be enlarged at will. While in Bitcoin Cash, for example, the blocksize has been increased by a factor of 8 (compared to Bitcoin) without any problems, a significantly larger block size is currently not practicable. This is because, the larger a block is, the longer it takes for it to be propagated by the worldwide blockchain network. This can have a negative effect for latency (the time it takes to distribute a new block to all nodes) and, also, security: More solutions to the puzzles are likely to be found as a certain block propagates through the network, splitting the honest miners' resources and, therefore, leaving the network more vulnerable to attack. Moreover, not every household can afford a high bandwidth and large hardware storage, so higher requirements can also lead to a lower degree of decentralization. This trade-off has already been discussed, e.g., in Bitcoin Magazine (2018). If, however, storage capacities (hard disks) and network speed continue to improve worldwide, a considerable increase in block sizes might be conceivable in the future. This would enable higher transaction rates without a noticeable increase in energy consumption.

Finally, for most PoW blockchains, the block reward is not constant, but periodically halved, typically, every few years. Since mining fees are currently negligible compared to block rewards, the upper bound (2) is proportional to the electricity price and block reward. Hence, if the prices for crypto-coins and electricity prices remain at the same level, one could even expect that in the long run, the energy consumption of PoW blockchains will also halve in each of these periods, until the rewards from mining are comparable to the total transaction fees.

We conclude that, although the energy consumption of PoW blockchains is arguably enormous in relation to their technical performance, it does not represent an essential threat to the climate, even if significantly more transactions are processed in the future. Moreover, since the area of application of most blockchains – and, in particular, the major cryptocurrencies – is often far beyond payments, plenty of opportunities for new ecosystems and business models arise. An evaluation should therefore not only compare performance metrics and energy consumption, but also take into account the unique opportunities offered by this technology.

3 Alternative Consensus Mechanisms

Fortunately, the PoW consensus mechanism, which – as already described – was designed to be energy-intensive, is not the only way to achieve consensus in a distributed system. The probably best-known alternative for the permissionless systems required for cryptocurrencies and other open decentralized applications is the so-called

Proof-of-Stake (PoS) consensus mechanism. In this case, the weight of a participant's vote is not tied to the scarce resource of computing power, but to the scarce resource of capital (see Sect. 2.1 on why coupling with a scarce resource is necessary). More precisely, there is a random mechanism (there are no truly random number generators for classical computers, but, as a first approximation, this heuristics provides a good indication. The pseudo-randomness typically comes from a subset of the previous blocks) that determines who is allowed to build ("mint", "forge", "bake") and attach the next block. With the help of this mechanism, the probability of being selected is linked to the amount of cryptocurrency that the node has deposited and locked ("staked") for this purpose. The deposit also incentivizes the node to stick to the rules of the network, as any misbehavior detected will lead to the node losing this deposit. The advantage of PoS is that it does not involve any computationally intensive steps such as solving the cryptographic puzzles in PoW. The computational complexity of PoS consensus is low and, typically, insensitive to network size. It is, therefore, very energy-efficient for large-scale systems. Accordingly, based on our arguments regarding the energy consumption associated with operating transactions in Sect. 2, the energy consumption of PoS blockchains is several orders of magnitude lower than that of PoW. It is primarily for this reason that the community of the cryptocurrency with the currently second-highest market capitalization, Ethereum, is trying to switch from PoW to PoS. Other cryptocurrencies, such as EOS, Tezos, and TRON – all of which feature in the Top 20 cryptocurrencies in terms of market capitalization – are already successfully using PoS. There are, however, controversial discussions in the community. Some argue that getting rid of PoW's energy consumption comes at the price of security, e.g., because one can only accrue voting weight (capital) from inside the system. However, one can also argue that PoS has less of a tendency to centralize (mining has economies of scale) and is, thus, more secure in the long run. We will not enter in this discussion up here but want to highlight that the outcome will likely decide which consensus-type for permissionless blockchains prevails and, therefore, impacts the energy consumption of future open decentralized applications.

On the other hand, blockchain technology can also be useful in constellations in which only a restricted group of participants take part in consensus. These are referred to as *permissioned* blockchains. They are of particular interest to many industries and, also, to the public sector: participants usually build a consortium, and there is a registration process meaning that all of the participants in consensus are known (Fridgen et al. 2018b; Rieger et al. 2019). Therefore, it is not necessary to tie voting weight to a scarce resource here, and one can reach consensus using some kind of election in which everyone has a single vote. Therefore, this kind of consensus mechanism is sometimes called Proof-of-Identity or, very often, Proof-of-Authority (PoA). The term PoA usually involves different levels of security, from mathematically proven and long-established, fully fault-tolerant mechanisms (Paxos, PBFT) over heuristically-secure algorithms, such as Istanbul BFT and Aura, to basic crash-tolerant mechanisms such as RAFT (De Angelis et al. 2017). Popular implementations of such permissioned blockchains are Hyperledger Fabric and Quorum. The more secure these PoA consensus mechanisms are, the greater their complexity and, therefore, the greater their energy consumption. For example, PBFT consensus overhead scales at least quadratically with respect to the number of nodes in the network and is hence – by contrast to PoW and PoS – highly sensitive on the network size. This, in turn, correlates with the energy consumption associated with consensus.

Beyond these popular consensus mechanisms, there are several more, an overview of which is provided by Eklund and Beck (2019). An example is Proof-of-elapsed-time, which intends to establish trusted random number generators through secure hardware modules. As PoS and PoA, these further concepts typically do not involve a cryptographic puzzle, except for some concepts which try to establish some kind of "useful Proof-of-Work" which solves puzzles that are in some way meaningful for business or science. Since many of these types of consensus mechanisms are not currently prevalent in relevant applications, and because they usually have low energy requirements compared to PoW, we will not investigate these consensus mechanisms in more detail.

The main result of the discussion about blockchains with alternative consensus mechanisms is that, by getting rid of energy intensity by design, their energy consumption is orders of magnitude lower compared to PoW-blockchains. Consequently, the energy consumption of non-PoW blockchains can hardly be considered problematic for the climate. Yet, beyond PoW and, thus, on a completely different scale, the type of consensus mechanism can have a significant impact on energy consumption.

4 The Impact of Redundancy on Energy Consumption

We have already seen that a portion of blockchains' energy consumption relates to consensus, and another portion relates to redundant operations. We have seen that for PoW blockchains, the energy consumption related to consensus outweighs the energy consumption associated with operating transactions, so the redundancy aspect is usually not discussed in detail. For non-PoW blockchains, however, the energy consumption related to consensus is no more

enormous, and, therefore, the contribution to total energy consumption by redundant operations may be significant. Hence, it is not only alternative consensus mechanisms that one should look at to further reduce the energy consumption of blockchain technology, but also concepts which allow reduced operation redundancy. Generally speaking, the primary motivations behind all of the concepts presented in this section that may help to reduce redundancy are increased scalability, throughput, and privacy for blockchain solutions. Conveniently, these all happen to reduce the degree of redundancy and, therefore, improve the overall energy consumption.

We can distinguish between two approaches to reducing redundancy: reducing the *degree* of redundancy, i.e., the number of nodes that perform certain operations, and the *workload* associated with operating a transaction. In attempts to reduce the degree of redundancy, a concept called *sharding* is often mentioned. Sharding is about splitting the nodes in the network into subsets ("shards") and processing each transaction on only one of these subsets. How easily sharding can be achieved largely depends on the consensus mechanism. For example, sharding is very difficult to apply to PoW blockchains, because one has to make sure that, within a shard, computing power is roughly equally distributed to maintain a balance of voting weight among the associated nodes. In a PoS blockchain, voting power is tied to the capital deposited by each node. This information is publicly available and can, therefore, be freely used in creation of shards. Other concepts to reduce the degree of redundancy include off-chain payment channels between two parties who repeatedly interact. Such channels usually require a transaction on the blockchain, in the course of which off-chain payment channels are created and terminated. Ideally, however, all interim transactions are operated purely bilateral and do not involve a transaction on the corresponding blockchain. That is to say that, ideally, only balances, or accumulated deltas signed by the members on the payment hub, are periodically recorded on-chain. Payment hubs, a generalization of payment channels to multiple parties, e.g., Nocust, or connections between them, e.g., Lightning for Bitcoin or Raiden for Ethereum, are the focus of active research (Gudgeon et al. 2019). A similar basic concept is the use of sidechains (e.g., Plasma for Ethereum). These are small blockchain networks which periodically refer to the main chain as a highly reliable root. Generally speaking, however, reducing the degree of redundancy also makes a blockchain network more centralized and must, therefore, be carefully weighed against concerns about security, liveness, and trust. Finding a good compromise between these interests could enable a reduction of the total workload in the system, and, therefore, a reduction of its total energy consumption.

On the other hand, the workload associated with redundant operations, e.g., the verification of new blocks, can be significantly reduced, which also mitigates the redundancy issue. One very straightforward improvement is, therefore, optimization of the computational complexity of the used cryptographic algorithms, e.g., for verifying signatures. Yet, this has some natural limits: Currently, transactions are operated "naively" on all nodes in the sense that all transaction-related data must be provided on-chain and all nodes recompute every step on their own. This could be significantly improved by storing and verifying only short correctness proofs on a blockchain and distributing the larger, plaintext data on another layer to the relevant participants. In particular, SNARKS, STARKS, and other (Zero-Knowledge-)Proofs of computational integrity which require much less verification and communication overhead on-chain seem very promising (Ben-Sasson et al. 2019). This is because, unlike methods that lower the degree of redundancy, these do likely not have a negative impact on security because every transaction is still verified by every node.

In summary, there are various ways to reduce the intrinsic redundancy of blockchains and, therefore, to reduce also their energy consumption. The relative energy saving potential is, however, negligible for PoW blockchains as the energy consumption of mining dominates all other contributions. However, it may still be relatively high for networks in which consensus is not energy-intensive, in particular, if the network is large.

5 A First Comparison of Different Architectures

We can now use our results from the previous chapters to make a first comparison of the energy consumption of typical blockchain architectures. The role of consensus has already been discussed in Sect. 3, where we suggested that a major distinction should be made between PoW and non-PoW blockchains, although the differences between other consensus mechanisms might also be significant. On the other hand, for small networks, redundancy does not add much absolute energy consumption, particularly when compared to the scale of PoW blockchains' energy consumption. By contrast, for large systems consisting of many nodes, the natural redundancy in a blockchain can lead to much higher energy consumption. If a PoS or alternative non-PoW blockchain replaces Bitcoin or another PoW cryptocurrency in the future, we have to expect that there will still be tens of thousands of nodes. Although the energy consumption of such a network will be negligible compared to Bitcoin, it will, therefore, remain high compared to a non-blockchain centralized system with minimal redundancy (i.e., because of backups). Figure 2

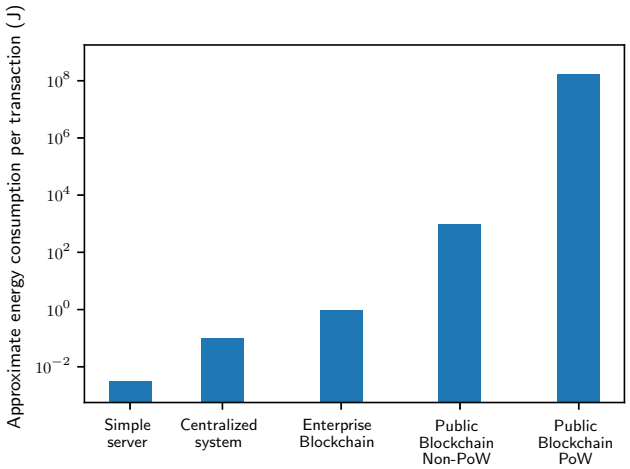

Fig. 2 A rough comparison of the order of magnitude of energy consumption per transaction for different architectures. A simple server can operate transactions with very low energy consumption. A typical non-blockchain, centralized system in applications will use a more complex database and backups, thus mildly increasing the energy consumption. A small-scale permissioned blockchain as used in cross-enterprise use-cases has a similar degree of redundancy, but some additional yet limited overhead due to, e.g., PoA consensus and more complex cryptographic operations. A non-PoW permissionless blockchain with a large number of nodes can already exhibit a significantly increased energy consumption due to the high degree of redundancy. However, compared to a major Proof-of-Work blockchain, energy consumption is still negligible

illustrates this observation and gives a rough comparison of the energy consumption of different architectures, using selected centralized systems as a baseline. We decided to display the energy per transaction. However, as discussed in Sect. 2, this is not an ideal metric for PoW blockchains but does correctly represent the order of magnitude.

We arrived at our estimates in the following way: A simple key-value store such as LevelDB can sustainably operate tens of thousands of transactions per second on office hardware with a power consumption of less than 100 W (own measurements), which yields less than 10^{-2} J per transaction. A more complex database, such as CouchDB, with one backup still manages more than 10^{3} transactions per second on the same hardware, resulting in at most 0.1 J per transaction (own measurements). As an example of a small-scale enterprise blockchain, we refer to a Hyperledger Fabric architecture with 10 nodes, each on cloud instances with 32 vCPUs and therefore likely consuming a few thousand Watts in total. According to Androulaki et al. (2018), such a system can handle around 3000 transactions per second, so we arrive at an order of magnitude of 1 J per transaction. On the other hand, an Ethereum full node on Geth which does not mine consumes approximately 0.1 J for a simple payment transaction, depending on whether or not idle power consumption is taken into account (own measurements). This seems low, but in a network of 10^{4} nodes, which is approximately the number of active full nodes in Bitcoin or Ethereum, this amounts to approximately 10^{3} J per transaction, which is already orders of magnitude more than for the described centralized systems and small-scale enterprise blockchain. However, it is still many orders of magnitude less than for the current PoW blockchains such as Bitcoin with about 10^{9} J per transaction. All numbers given here should be taken with caution as they are highly dependent on the precise architecture, security measures, type of hardware, and other parameters. They should therefore be regarded a ballpark estimate, and reliable numbers have yet to be established. We suggest this interesting topic for further work, including a more thorough investigation of the role of consensus mechanism and the energy efficiency of transactions depending on transaction type or choice of blockchain implementation. For permissioned blockchains, this might be particularly relevant when enterprises have to decide for or against a particular blockchain implementation.

6 Conclusion

In this article, we first analyzed the energy consumption of today's prevailing PoW blockchains, which underly most cryptocurrencies. While their energy consumption is, indeed, massive, particularly when compared to the number of transactions they can operate, we found that they do not pose a large threat to the climate, mainly because the energy consumption of PoW blockchains does not increase substantially when they process more transactions. We also argued that although the energy consumption of non-PoW blockchains and in particular permissioned blockchains which are used in enterprise context is generally considerably higher than that of non-blockchain, centralized systems, it is many orders of magnitude lower than that of PoW cryptocurrencies such as Bitcoin. We also observed a close interrelationship between security aspects and the choice of consensus mechanism and redundancy characteristics, and therefore, energy consumption. Hence, we conclude that further investigation in this direction, which has many similarities to Vitalik Buterin's "scalability trilemma", might help to find the best compromise between performance, security, and energy consumption.

Our contribution demonstrates that the energy consumption of blockchain technology differs significantly between different design choices. Consequently, it is an important dimension to consider during the conception of a blockchain-based IT solution (Kannengießer et al. 2019). We argued that using blockchain technology with non-PoW consensus – which is the case in an increasing

number of business applications – already substantially mitigates sustainability issues. However, we also illustrated that due to consensus and inherent redundancy, blockchain-based solutions in general still require more energy than non-blockchain, centralized architectures. However, in enterprise applications, blockchains are typically only one part of a hybrid solution in which most processes are operated via conventional IT, and little information which is relevant to the remaining participants on the blockchain is processed on-chain (Rieger et al. 2019). Reducing the workflows operated on-chain to a minimum, therefore, also mitigates concerns about the energy consumption. On the other hand, we know from other areas of IT that significant energy savings can be enabled by process optimization and digitization. As there are plenty of scenarios in which blockchain technology might finally turn out to be an enabler of the further digitization of processes, the increase in energy consumption of a specific blockchain must always be weighed against the savings it provides. For example, by enabling the digitization of supply-chain processes, blockchain can substantially reduce the amount of paperwork and transport, including air-freight (Jensen et al. 2019), or allow for more targeted recalls, leveraging many opportunities to reduce carbon emissions.

However, we still lack reliable information on the detailed energy consumption of different non-PoW blockchains. We also lack information on the quantification of their energy-saving potential for specific use-cases. Together, these remain a field for future work, which will involve a more detailed analysis of the role of consensus, as well as transaction-based overheads and efficiency, for a large subset of the consensus mechanisms and blockchain implementations available. It will also involve a discussion about the compromise between the degree of decentralization, security, performance, energy consumption, and further metrics which are of importance for blockchain-based use-cases. Based on such investigations and more reliable numbers, and the development of the most influential blockchain use-cases in practice, we will finally be in a position to decide whether or not the energy consumption of blockchain technology outweighs the savings in a specific scenario.

Acknowledgements Open Access funding provided by Projekt DEAL. This work was supported by PayPal and the Luxembourg National Research Fund FNR (P17/IS/13342933/PayPal-FNR/Chair in DFS/Gilbert Fridgen. We also thank André Luckow, Alexander Rieger, and the anonymous reviewers for their valuable comments and support.

References

Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, Enyeart D, Ferris C, Laventman G, Manevich Y, et al. (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth eurosys conference, pp 1–15

Beck R (2018) Beyond bitcoin: the rise of blockchain world. Computer 51(2):54–58

Beck R, Avital M, Rossi M, Thatcher JB (2017) Blockchain technology in business and information systems research. Bus Inf Syst Eng 59(6):381–384

Beck R, Müller-Bloch C, King JL (2018) Governance in the blockchain economy: a framework and research agenda. J Assoc Inf Syst 19(10):1020–1034

Beincrypto (2020) Bitcoin's hash rate retraces 40% this month, slips under 100 ehash/s. https://beincrypto.com/bitcoins-hash-rate-retraces-40-this-month-slips-under-100-ehash-s/. Accessed 26 Mar 2020

Ben-Sasson E, Bentov I, Horesh Y, Riabzev M (2019) Scalable zero knowledge with no trusted setup. In: Annual international cryptology conference, pp 701–732

Bitcoin Magazine (2018) What is the bitcoin block size limit? https://bitcoinmagazine.com/guides/what-is-the-bitcoin-block-size-limit. Accessed 05 Feb 2020

Buhl HU, Jetter M (2009) BISE's responsibility for our planet. Bus Inf Syst Eng 1(4):273–276

Coinmarketcap (2020) Top 100 cryptocurrencies by market capitalization. https://coinmarketcap.com/. Accessed 05 Feb 2020

Coinswitch (2019) Bitcoin mining hardware. https://coinswitch.co/news/top-10-best-bitcoin-mining-hardware-in-2020-latest-review-and-comparison. Accessed 05 Feb 2020

Crosby M, Pattanayak P, Verma S, Kalyanaraman V et al (2016) Blockchain technology: beyond bitcoin. Appl Innov 2:6–19

De Angelis S, Aniello L, Lombardi F, Margheri A, Sassone V (2017) Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain. https://eprints.soton.ac.uk/415083/2/itasec18_main.pdf. Accessed 05 Feb 2020

De Vries A (2018) Bitcoin's growing energy problem. Joule 2(5):801–805

Dittmar L, Praktiknjo A (2019) Could bitcoin emissions push global warming above 2°C? Nat Clim Change 9(9):656–657

Douceur JR (2002) The sybil attack. In: International workshop on peer-to-peer systems, pp 251–260

Eklund PW, Beck R (2019) Factors that impact blockchain scalability. In: Proceedings of the 11th international conference on management of digital ecosystems, pp 126–133

Eyal I, Sirer EG (2014) Majority is not enough: Bitcoin mining is vulnerable. In: International conference on financial cryptography and data security, pp 436–454

Fridgen G, Lockl J, Radszuwill S, Rieger A, Schweizer A, Urbach N (2018a) A solution in search of a problem: a method for the development of blockchain use cases. In: 24th Americas conference on information systems, pp 1–10

Fridgen G, Radszuwill S, Urbach N, Utz L (2018b) Cross-organizational workflow management using blockchain technology-towards applicability, auditability, and automation. In: Proceedings of the 51st Hawaii international conference on system sciences, pp 3507–3516

Georgiadis E (2019) How many transactions per second can bitcoin really handle? Theoretically. Cryptology ePrint Archive, Report 2019/416, https://eprint.iacr.org/2019/416. Accessed 05 Feb 2020

Gudgeon L, Moreno-Sanchez P, Roos S, McCorry P, Gervais A (2019) SoK: off the chain transactions. https://pdfs.semanticscholar.org/4d5b/9fb1c4205b61060117e3c71b04464c2a1c77.pdf. Accessed 5 Feb 2020

Jensen T, Hedman J, Henningsson S (2019) How tradelens delivers business valuewith blockchain technology. MIS Q Exec 18(4):221–243

Kannengießer N, Lins S, Dehling T, Sunyaev A (2019) What does not fit can be made to fit! Trade-offs in distributed ledger technology designs. In: Proceedings of the 52nd Hawaii international conference on system sciences

Krause MJ, Tolaymat T (2018) Quantification of energy and carbon costs for mining cryptocurrencies. Nat Sustain 1(11):711–718

Labazova O, Dehling T, Sunyaev A (2019) From hype to reality: a taxonomy of blockchain applications. In: Proceedings of the 52nd Hawaii international conference on system sciences

Lockl J, Schlatt V, Schweizer A, Urbach N, Harth N (2020) Toward trust in internet of things (IoT) ecosystems: design principles for blockchain-based IoT applications. IEEE Transact Eng Manag, to appear

Mora C, Rollins RL, Taladay K, Kantar MB, Chock MK, Shimada M, Franklin EC (2018) Bitcoin emissions alone could push global warming above 2°C. Nat Clim Change 8(11):931–933

Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. Accessed 05 Feb 2020

O'Dwyer KJ, Malone D (2014) Bitcoin mining and its energy footprint. In: 25th IET Irish signals & systems conference 2014, pp 280–285

Rieger A, Guggenmos F, Lockl J, Fridgen G, Urbach N (2019) Building a blockchain application that complies with the EU general data protection regulation. MIS Q Exec 18(4):263–279

Schmidt NH, Erek K, Kolbe LM, Zarnekow R (2009) Sustainable information systems management. Bus Inf Syst Eng 1(5):400–402

Stoll C, Klaaßen L, Gallersdörfer U (2019) The carbon footprint of bitcoin. Joule 3(7):1647–1661

Truby J (2018) Decarbonizing bitcoin: law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies. Ener Res Soc Sci 44:399–410

Vranken H (2017) Sustainability of bitcoin and blockchains. Curr Opin Environ Sustain 28:1–9