Energy Efficiency of Blockchain Technologies

About this report

This is the third thematic report prepared by the new team leading the EU Blockchain Observatory and Forum, aiming to present the latest updates and developments within the EU blockchain ecosystem.

This is the part of a series of reports that will be published addressing selected topics in accordance with the European Commission priorities. The aim is to reflect on the latest trends and developments and discuss the future of blockchain in Europe and globally.

Credits

This report has been produced by the EU Blockchain Observatory and Forum team. Written by:

- Ioannis Vlachos, Nikos Kostopoulos, Tonia Damvakeraki, INTRASOFT International
- Zalan Noszek, Bitfury
- Iordanis Papoutsoglou, Kostas Votis, CERTH
- Alexi Anania, Marianna Belotti, Ismael Arribas, EU Blockchain Observatory and Forum Expert Panel
- Wendell Cathcart, Energy Web
- Tadej Slapnik, HashNET
- Orestis Papageorgiou, Gilbert Fridgen, SnT - Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg
- Johannes Sedlmeir, FIM Research Centre, University of Bayreuth

Special thanks to Scope for the editorial review and language proofing

Note

While we have done our best to incorporate the comments and suggestions of our contributors where appropriate and feasible, all mistakes and omissions are the sole responsibility of the authors of this paper.

Disclaimer

Contents

Section 1: Demystifying Consensus Protocols 6

INTRODUCTION 6

OVERVIEW OF VARIOUS METHODOLOGIES 6

ENERGY EFFICIENCY OF CONSENSUS PROTOCOLS 10

Energy Consumption of the Energy Web Blockchain 18

HashNET Blockchain - Overcoming Scalability and Performance Barriers 19

Section 2: Blockchain Energy Consumption Indices 22

OVERVIEW OF VARIOUS METHODOLOGIES 22

The Cambridge Bitcoin Electricity Consumption Index (CBECI) 23

Existing/Future Extensions of the methodologies to calculate electricity consumption of other blockchains. 23

Evaluation of Energy Consumption of Proof-of-Stake Blockchains 25

Section 3: Blockchain Performance 27

Blockchain Performance Comparison 27

Comparison of Cryptocurrency Mining Infrastructure 33

Section 4: View from the Industry 38

Interview with Walter Kok, CEO, Energy Web 38

Section 5: Decarbonising Blockchains 42

INTRODUCTION 42

HOW TO DECARBONISE BLOCKCHAINS 43

THE PATH FORWARD 45

Section 6: Policy Recommendations 46

Recommendations 46

Reference List 48

Annex 50
Comparison of Consensus Protocols 50

Executive Summary

The purpose of this thematic report is to present an updated view of the aspects related to the energy efficiency of blockchain technologies. The topic of energy consumption of blockchains and especially of the Bitcoin blockchain has recently triggered a lot of discussions and a debate has started on the topic of making Bitcoin a sustainable ecosystem.

Although the Bitcoin is currently in the spotlight, this thematic report does not only focus on Proof-of-Work blockchain solutions, but also analyses the whole spectrum of blockchain technologies. In this respect the various consensus mechanisms are analysed with regards to their energy consumption, but also other aspects of the consensus protocols are taken into account, such as security and throughput, that are deemed important when considering the application of blockchain solutions in real-world use cases.

With regards to the energy efficiency of blockchain technologies, the thematic report presents the various approaches and methodologies that address the challenge of estimating the energy consumption of the Bitcoin blockchains. It should be mentioned that although the report is focusing upon the whole spectrum of consensus mechanisms, due to the high energy consumption of Bitcoin blockchain, only methodologies that analyse the energy consumption of the Bitcoin are available and, thus, covered in the report.

Apart from the various diverse applications of blockchain technologies across several sectors ranging from finance and supply chain to the pharmaceutical and energy sectors, cryptocurrencies on the various blockchains are constantly under the spotlight. To also address the topic of cryptocurrencies, the thematic report also deals with the topic of the energy efficiency of the ICT infrastructure that is used for cryptocurrency mining.

In the shade of the high energy consumption of the Bitcoin blockchain issue, the issue for a more sustainable model for Bitcoin and other Proof-of-Work blockchains is once more on the table. Given the fact that the technologies underpinning crypto are powered by electricity—just like other electricity-powered technologies such as cloud computing, data storage & processing, social networks, and artificial intelligence, industries from across the global economy are beginning to decarbonise their operations as a means to facilitate widespread, sustainable industry growth. In this context, the report also focuses on the most recent initiative for decarbonising the cryptocurrency scene. Inspired by the Paris Climate Agreement, the Crypto Climate Accord was launched as a private sector-led initiative for the entire crypto community focused on decarbonising the cryptocurrency industry in record time.

From the analysis performed within the report to the topics related to the energy efficiency of blockchain technology, a set of recommendations were derived. On the energy efficiency side, at the EU level, the European Blockchain Services Infrastructure needs to consider the energy consumption (and efficiency) of blockchain when deciding on the underlying technology for developing the necessary digital infrastructure. Another aspect closely related to energy efficiency is the scalability and performance of blockchain solutions. Therefore, it is recommended that energy efficiency-related issues need always to be treated along with the scalability and performance requirements of the blockchain-based solution under evaluation. Moreover, to compensate the excess energy consumption especially of Proof-of-Work blockchains, it is important to make sure that renewable energy is used to the maximum possible extent to cover the demand of energy of blockchain-based solutions. Other aspects that are related to the energy consumption of blockchain technology are the recommendation for certification of equipment used as infrastructure for the deployment of public-sector blockchain solutions at a European and Member State level, as well as the introduction of specific evaluation criteria related to the performance and energy efficiency of blockchain-based solutions for the public sector need to be specified at European and Member State level. Finally, it is recommended that to assess the energy consumption of blockchain-based solutions in an independent and unbiased manner, a blockchain energy consumption index should be developed and agreed upon between the Member States, as well as knowledge-sharing and dissemination of pilot results and best practices on blockchain deployments between the Member States should be fostered.

To offer a more spherical view of the topic of energy efficiency of blockchain technologies, the thematic report approaches this interesting topic both from an academic (research and development) and an industrial approach. The thematic report is organised as follows. Section 1 presents an overview of the various consensus mechanisms and discusses their respective characteristics. Section 2 presents a deep dive into the topic of the Bitcoin energy consumption indices and analyses the different methodologies and approaches currently developed. Section 3 presents an in-depth analysis of the energy consumption and performance of the cryptocurrency infrastructure, while Section 4 presents the industry's view on the topic of scalability and performance of blockchain solutions. Finally, the Crypto Climate Accord initiative for decarbonising the crypto space is presented in Section 5, while the policy recommendations on the topic are discussed in Section 6.

Section 1: Demystifying Consensus Protocols

INTRODUCTION

Energy efficiency (or energy consumption) of blockchain solutions is highly related to the underlying mechanism that is used for achieving consensus between the nodes of the network. Currently, blockchains that are based on the Proof-of-Work, such as Bitcoin and Ethereum, are characterised by high energy consumption. Especially in the case of Bitcoin, there are currently several ongoing discussions on the amount of energy consumed by the miners of the network. The purpose of this section is to present an introduction to consensus mechanisms and describe their respective characteristics. Apart from the energy-demanding Proof-of-Work blockchains, it can be seen that there are several other approaches to achieve consensus. These approaches guarantee both the required level of security and trust, being at the same time energy-efficient and allowing for the scalability and performance of the applications based on them. Such alternatives are the Proof-of-Stake and Proof-of-Authority consensus mechanisms.

OVERVIEW OF VARIOUS METHODOLOGIES

Generally, “consensus” refers to the process of achieving agreement among different actors operating in a system. More precisely, “blockchain consensus” denotes the procedures through which the different participants of a blockchain network agree on a specific state of data on the system referred to as the correct state.

Participation Modes

Differently from a traditional database where only a single entity, the owner or the administrator, keeps a copy of the database, distributed ledgers foresee multiple entities to hold a personal copy of the underlying database (i.e., ledger). This new paradigm is based on the replication of data and the distributed storage by the different nodes of the blockchain networks (i.e., the blockchain peers). Due to the distributed storage, ensuring that all networks’ nodes achieve an agreement on a common state represents a difficult task. The vision of the ledger may not be the same for all the nodes as changes on the ledgers (i.e., data updates) have to be propagated to all other peers in the network. Consensus leads to a common truth, hence a consensus protocol: (i) ensures that the data on the ledger is the same for all network nodes, and (ii) prevents malicious actors from manipulating such data.

Two main modes for operating on a blockchain exist: “*permissionless”* and “*permissioned”*. These two ways of operating concern at first the access to the blockchain network and secondly the participation in the agreement procedure (consensus) responsible for maintaining the state of a blockchain system. What in literature is often referred to as *public* and *private* blockchains denote just the access to the network. Whenever there is open access, anybody is allowed to access the network and to observe (i.e., read) the data ledger. On the other hand, if access is permissioned only whitelisted participants have the rights to access the network. Concerning the participation in the ledger maintenance procedures, i.e., consensus, whenever it is open to anyone blockchain are called permissionless. Whenever permissions are in place, the system may either restrict on only writing (validation) rights, or on both reading (access) and writing rights. In the first case, the ledger is publicly readable, but any modification of the transaction ledger is entrusted to a selected set of nodes (i.e., *open-permissioned* distributed ledgers). In the so-called *full-permissioned* distributed ledgers participants are selected in advance and all network activities are restricted to these actors only. Fig. 1.1 reports the different participation modes that differentiate between less decentralised distributed ledgers (generally embedding permissions) and those that additionally offer disintermediation namely, that cut out any middleman (i.e., permissionless distributed ledgers).

Source: M. Belotti et al. "A vademecum on blockchain technologies: When, which, and how." IEEE Communications Surveys & Tutorials 21.4 (2019): 3796-3838.

Consensus Protocols

Consensus problems make multi-agent systems converge to a common vision and it leads all network agents to share the same data. Hence, consensus protocols on blockchains:

(i) ensure that the data on the distributed ledgers is the same for all network actors, and

(ii) prevent faulty nodes (acting both rationally and irrationally) from manipulating the data.

The consensus mechanisms vary between different blockchain implementations according to the system nature (permissionless and permissioned). A variety of consensus protocols exist, with currently three main classes:

- Proof-of-X (PoX) consensus protocols
- Byzantine Fault Tolerant (BFT) protocols
- Hybrid consensus protocols

The first two classes characterise consensus in blockchains while algorithms defined as ‘hybrid’ mix protocols’ aspects from the first two classes. The recent complex consensus implementations proposed by new blockchain platforms consist in creative combinations of PoX and BFT protocols.

Consensus in distributed systems has been studied long before Bitcoin’s birth and the very first class of consensus protocols was one of “BFT algorithms”. **BFT algorithms** (a class of State Machine Replication protocols) were adopted to deal with Byzantine nodes i.e., rational nodes acting maliciously. These types of protocols are based on voting procedures where network agents are called to accept or reject a specific vision of the network’s state. BFT protocols generally work in systems with a limited number of participants since according to these protocols consensus *proposal* and consensus *decision* represent two separate events demanding the different system’s participants to communicate with each other. Indeed, communication complexity represents the major downside of this protocol class. Hence, the necessity for closed-system adoption such as permissioned blockchains.

The advent of Bitcoin gave rise to a new technology based on a new innovative consensus protocol called Proof-of-Work (PoW). The idea behind PoW consensus was to gain the right to validate the state of the ledger by proving to have worked from a computational point of view i.e., to have used a machine (e.g., a computer) to work for the system. This idea of gaining the right to propose and validate the agreement value proposed by the PoW consensus was really innovative at the time since it gave to every node a chance to have a deciding role in the system. This gave rise to the larger category of Proof-of-X (PoX) consensus algorithms where X denotes the resource a network node is consuming/allocating to gain the right to propose and validate the agreement value. While in Bitcoin the X stands for "computational resources" for other consensus mechanisms it stands for a "stake" of the system (Proof-of-Stake), or memory "capacity" (Proof-of-Capacity) or again wireless network "coverage" (Proof-of-Coverage). All these alternative

PoX-schemes try to replace the energy consumption implicated by the PoW consensus by the consumption of alternative resources.

The advent of permissioned participation modes and the raise of permissioned blockchains and DLTs make the industry reconsidering traditional BFT. Here blockchains are no more peer-to-peer (P2P) systems where every node is given the chance to participate in the consensus of a blockchain but blockchains can be closed systems as the traditional distributed ones studied in the XX century. This consensus phase is marked by protocol experimentation with BFT-based algorithms with the aim of preserving permissionless consensus while keeping the process efficient by reducing the number of participating nodes to the consensus. Hence, consensus is divided in two phases; the first one that determines the formation of a committee of voters elected through a PoX mechanism and the second one where nodes vote according to BFT consensus.

CONSENSUS EVOLUTION

Agreement problems saw abundant applications in complex systems since the 1980s. Hence, consensus problems existed prior to blockchain and therefore specific consensus protocols have been proposed to deal with blockchains and DLTs. A digression might be opened regarding consensus evolution and the three types of distributed ledgers with the permissionless/permissioned nature of a DLT.

Consensus theory evolved from the pre-Bitcoin phase to the post-Bitcoin one, introducing a new category of protocols i.e., the PoW consensus protocols. The second evolution of consensus took place when Bitcoin gave the way to blockchain i.e., when other blockchains were proposed and Bitcoin was anymore a solo player in the ecosystem. This second phase corresponded with the birth of the second generation of blockchains adopting PoX schemes; alternatives to Bitcoin's PoW. A third evolution was characterised by the advent of permissioned participation modes and the raise of permissioned blockchains and DLTs. Here blockchains are no more peer-to-peer (P2P) systems where every node is given the chance to participate in the consensus of a blockchain but blockchains can be closed systems as the traditional distributed ones studied in the XX century. The consensus then evolved by reconsidering traditional BFT and by implementing such protocols in blockchains now considered as a branch of DLTs (i.e., a DLT structured as a chain of transaction blocks). The fourth evolution step was marked by consensus experimentations with BFT-based algorithms aiming to preserve permissionless consensus while keeping the process efficient by reducing the number of participating nodes to the consensus. Hence, the consensus is divided into two phases; the first one determines the formation of a committee of voters elected through a PoX mechanism and the second one where nodes vote according to BFT consensus.

The four consensus evolution steps mark the five phases of consensus theory represented in Figure 3.2 characterising the main consensus variants for each consensus class. Main algorithms representing the classes are associated to each consensus variant.

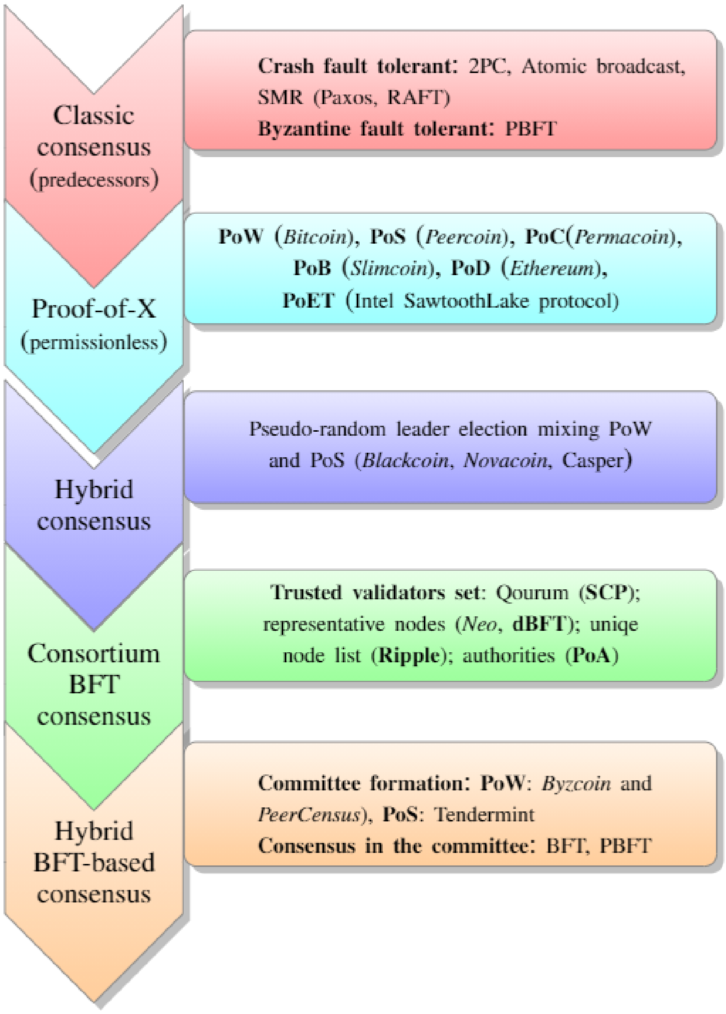


Fig. 3.2: Evolutionary route of consensus protocols in five classes: (i) Classic consensus, (ii) Proof-of-X consensus, (iii) Hybrid consensus, (iv) Consortium BFT consensus and, (v) Hybrid BFT-based consensus. Source: M. Belotti et al. "A vademecum on blockchain technologies: When, which, and how." IEEE Communications Surveys & Tutorials 21.4 (2019): 3796-3838.

ENERGY EFFICIENCY OF CONSENSUS PROTOCOLS

In recent years, the term ‘blockchain’ has often been used synonymously with inefficiency and disproportionate energy consumption. These claims often point to a single component of the technology, the consensus mechanism. However, blockchain technology is not homogenous, and the amount of energy consumed by different consensus mechanisms varies by several orders of magnitude. Moreover, contrary to often heard statements, energy consumption does not necessarily grow with the number of transactions executed. This section aims to provide an overview of a subset of the available consensus mechanisms and their role in different blockchains while placing emphasis on their energy consumption and the parameters that influence it. Considering the large number of consensus mechanisms and their minor variations, we focus on those utilised by well-known blockchains and widely used in the industry and public sector.

A blockchain is a distributed system not controlled by a distinguished operator that maintains an append-only, ordered list of transaction records. Transaction records are disseminated, ordered, and batched in blocks through a distributed protocol followed by the participating nodes. This establishes a synchronised distributed database. We classify blockchains as permissioned or permissionless, based on who is eligible to become an entity that can actively participate in the decision-making on which blocks to append (Butijn et al., 2020). Another frequent classification distinguishes between public blockchains, where running a node for submitting, validating, and reading transactions is allowed to anyone, and private blockchains, where access is restricted.

Permissioned blockchains are often used by consortia in the public or private sector. Organisations that wish to participate in the operation of a permissioned blockchain must typically fulfill criteria specified by the existing nodes in the network. Some of these requirements include, for instance, an identity verification process, uptime-, hardware-, or bandwidth-specifications for the nodes, or a period where the node establishes trust with other nodes in the system. Typically, the participating entities are companies or public organisations that have sufficient resources to provide significant computing, storage, and bandwidth requirements. As the total number of entities is known, decisions regarding which blocks to append can be made based on a voting-like protocol. This also implies that the waiting time for getting a sufficient number of votes can be controlled. Hence, permissioned blockchains tend to feature faster transaction speeds and are less susceptible to malicious users attempting to sabotage the network. The higher throughput and additional level of security are two of the primary reasons that make permissioned blockchains the choice for many private blockchains, besides restricted data visibility and a higher degree of control of governance and transaction fees.

On the other hand, permissionless blockchains allow for unrestricted access and participation. As a result, they tend to have a larger userbase which makes them more decentralised. However, this generally comes at a substantial latency cost since additional mechanisms are necessary to ensure that malicious users do not hijack the system. Elections based on “one participant, one vote” are not feasible here, because there is no control on how many accounts a participant generates. Consequently, protection against “Sybil attacks” where an adversary creates a large number of accounts to outvote the system is required. The open participation in the network's operations makes public permissionless blockchains suitable for cryptocurrencies.

Despite their differences, both types of blockchains have a few core concepts in common. One of them is that trust in a blockchain protocol should not be bestowed on a single or a relatively small group of nodes, and that the nodes always reach a unique decision even when some of them crash or behave maliciously. To achieve these objectives, blockchains employ a crash fault-tolerant (which may be sufficient for a private blockchain where participants know each other and can be held accountable for misbehavior via legal contracts) or byzantine fault-tolerant consensus mechanism (which is a de-facto requirement for permissionless blockchains).

PERMISSIONED CONSENSUS

When it comes to permissioned blockchains, the consensus mechanism can be compared to a voting-based protocol where every user has a pre-defined voting weight. Typically, the different participants have equal voting power. However, a reputation-based weighting is also possible and can be useful if there is some soft hierarchical structure (imagine OEMs and small suppliers in a supply chain network, where a single supplier's vote should arguably not have the same weight as an OEM's, but a considerable number of suppliers should still be able to outvote the OEM). This kind of mechanism is often called Proof-of-Authority (PoA), although this is an umbrella term including mechanisms with different properties and levels of security (De Angelis et al., 2017). These mechanisms can be separated into crash fault-tolerant (CFT) and byzantine fault-tolerant (BFT) mechanisms.

CFT consensus mechanisms divide the network's nodes into two main categories: follower nodes and – at any time – a single leader node. The follower nodes elect the leader, interact exclusively with the leader after its election, and the leader is the sole entity responsible for ordering and committing new transactions to the blockchain. The mechanism utilises a two-phase commit protocol (2PC) which operates as follows: In the first phase (commit-request phase), the leader communicates with the follower nodes to ensure they are ready to commit a transaction. On the second phase (commit phase), the leader commits or aborts the transaction, broadcasting the action to the followers. When the leader crashes, a new leader is elected, and through the two-phase "gradual" commit, conflicts that may arise (for instance, if the previous leader notified only a subset of the other nodes to commit before it crashed) can be resolved. CFT consensus mechanisms can operate while most nodes have not crashed but cannot cope with malicious nodes, as the followers blindly "follow" the leader as long as it is running. As a result, CFT consensus mechanisms should be used only in blockchains with a high level of trust or at least accountability between nodes, or if some degree of fault-tolerance against malicious behavior is achieved on another level (e.g., in Hyperledger Fabric). Probably the most widely used CFT consensus mechanism is RAFT (Ongaro and Ousterhout, 2014). Some of the properties that make RAFT appealing to private blockchains include fast block times (as low as 50 ms if network latency is small, e.g., a regional network), transaction finality (transactions cannot be altered retrospectively), and the fact that it does not generate empty blocks. Blockchains that use RAFT include GoQuorum and Hyperledger Fabric.

In contrast, BFT consensus mechanisms can deal with malicious activity, allowing a blockchain to remain operational as long as more than 2/3 of the nodes remain honest and available. The mechanism achieves that by adding an extra phase, creating a three-phase commit protocol (3PC). The extra phase (pre-commit phase), sandwiched between the two previously mentioned phases, allows nodes to determine whether enough other nodes are planning to commit or not before they actually commit a transaction. Because the third phase adds an extra round of message exchange between the nodes, it contributes to higher latency and increased bandwidth requirements. This makes BFT mechanisms generally slower than CFT mechanisms. Some of the most common BFT based consensus mechanisms are IBFT 2.0 (Saltini and Hyland-Wood, 2019) and QBFT used by Hyperledger Besu and RBFT (Aublin et al., 2013) used by Hyperledger Indy which are all based on PBFT (Castro and Liskov, 1999). Like in CFT, these mechanisms achieve immediate finality (assuming the network has more than three nodes), but the time it takes to add new blocks increases as the number of nodes grows. Consequently, BFT consensus can become challenging for large networks that consist of hundreds of nodes.

PERMISSIONLESS CONSENSUS

When it comes to permissionless blockchains, a basic one-user one-vote protocol is infeasible; under the veil of anonymity or at least pseudonymity, a user could create multiple accounts at essentially no cost and outvote the system ("Sybil attack"). To avoid this issue, permissionless blockchains associate each user's voting power with a scarce resource that cannot be replicated without considerable costs and whose possession can be proven to the network (Sedlmeir et al., 2020a). The costs for the scarce resource should be linearly dependent on the voting weight and bound to a specific account. As a result, account splitting would become useless. Moreover, avoiding economies of scale that would give an advantage to participants that already have a lot of voting power would ensure fairness.

In Proof-of-Work (PoW), the scarce resource is the computational power of each user. In this mechanism, nodes compete for the solution of a computationally expensive and – as a result – energy-intensive, cryptographic puzzle ("mining"). The winner of the competition gets to create the next block and receives a specific amount of the blockchain's native currency and fees for the transactions included in this block as a reward. This mechanism makes it practically impossible for malicious users to tamper with the blockchain after some time, as changing one block would require tremendous amounts of computational power to "outrun" the rest of the system for this time period. Additionally, it places a high economic risk because the resources invested into mining a block would likely be wasted when the next, likely honest miner does not accept the block and prefers to build on an alternative block instead. The complexity of the cryptographic puzzle increases as more mining power is present to keep the average time between new blocks at a constant level and, thus, to ensure stable functionality. Mining power, in turn, is driven by the economic incentives given through block rewards (which are proportional to the current price for the cryptocurrency) and transaction fees. As cryptocurrency prices have significantly increased over the last years, it seems that PoW has become more and more computationally demanding over time, but this may not hold forever. Notably, the regular halvings of block rewards, as implemented in many PoW cryptocurrencies such as Bitcoin (Nakamoto, 2008), would even reduce the energy consumption in the long run, given constant prices and transaction fees. In the early stages, when incentives and the puzzle's complexity are low, power is fairly distributed among the blockchain's participants ("one CPU, one vote"), but as the complexity rises, rich users benefit increasingly from economies of scale (electricity and specialised hardware cost increase sublinearly), and there is a substantial risk that power gets accumulated by a few groups of users. This can be observed, for instance, in Bitcoin in the form of large mining pools. PoW is one of the most commonly used consensus mechanisms for permissionless blockchains and to date used by Bitcoin, Ethereum (Buterin, 2014), Monero, Zcash, and many more.

Another popular consensus mechanism for permissionless blockchains is Proof-of-Stake (PoS), in which the scarce resource is each user's share of the blockchain's native currency. While this mechanism is considerably less energy demanding than PoW and seems to provide comparable security guarantees, the initial coin allocation is critical since poor initial distribution can result in the permanent concentration of power. There are three main variations of PoS mechanisms, Pure Proof-of-Stake (PPoS), Delegated Proof-of-Stake (DPoS), and Bonded Proof-of-Stake (BPoS). They have in common that the probability of creating the next block is proportional to the number of coins held (or received by delegation). Consequently, remuneration corresponds to interest at a rate that is – on average – the same for every participant. While rich users get more rewards in absolute figures, their relative stake and, thus, their voting weight does not change over time. This likely avoids the long-term centralisation tendencies observed in PoW (Roşu and Saleh, 2021).

PPoS, used for instance by Algorand (Gilad et al., 2017), allows any user to be selected as a leader or a committee member, where the likelihood of selection is proportional to the number of coins held by the user. Following the selection, the leader proposes the next block. Next, the committee members vote on whether to commit the block in a voting-based, BFT-like protocol. After the creation of the block, a new round starts, and new members are selected. This approach makes it difficult for malicious users to attack committee members because they do not foresee who will be chosen as leader or committee members next. Although rich users have a higher chance of being selected, dishonest activity on their side would diminish the value of the currency they have heavily invested in, which acts as a deterrent.

Used by EOS and TRON, for instance, DPoS allows users to elect a specific number of delegates with voting power proportional to the coins they are holding. Following their election, delegates take turns creating the next blocks. The difference with PPoS is that delegates stay in power for extended periods of time and are not re-elected after each block. This mechanism allows for higher throughput as the hardware and bandwidth requirements on delegates can be increased. However, it also comes at the expense of decentrality since, at any point, only a handful of delegates have power over the system. Additionally, this mechanism could expose the delegates to denial-of-service attacks that would cause the blockchain to stall; consequently, being a delegate is challenging.

In BPoS, used for example by Ethereum 2.0 and RChain, users can lock a portion of their balances for a certain period of time, and the probability of being chosen as the next validator is proportional to the number of coins they have locked. The selected users, after creating the block, receive the transaction fees as a reward. The mechanism prevents users from behaving maliciously by burning the locked coins in the event of fraudulent activity. Since this mechanism does not incentivise, and in some cases does not allow users with small amounts of coins to lock their balances, it enables rich users to accumulate more wealth over time, potentially damaging the decentrality of the blockchain.

It is important to note that this classification is not exhaustive, and there are PoS mechanisms combining ideas from different categories. One of them is Ouroboros Praos (David et al., 2018), used by Cardano, in which users are not required to lock any amount of their balance, they can be selected as leaders based on the number of tokens they hold (there is no committee like in PPoS). They also have the option to delegate their power to another user if they choose. Additionally, the distinction between permissioned and permissionless consensus is not as clear as it may seem. For example, although highly theoretical at this point, a voting-based consensus mechanism built on a certificate-based European digital identity (European Commission, 2021) could potentially provide similar security characteristics like PoS while avoiding the aggregation of voting power by the wealthy and keeping a low eligibility threshold, making it accessible to all citizens. This mechanism is technically permissioned, but because of the low entrance criterion, it may be much closer to permissionless than to permissioned systems with high-end hardware criteria.

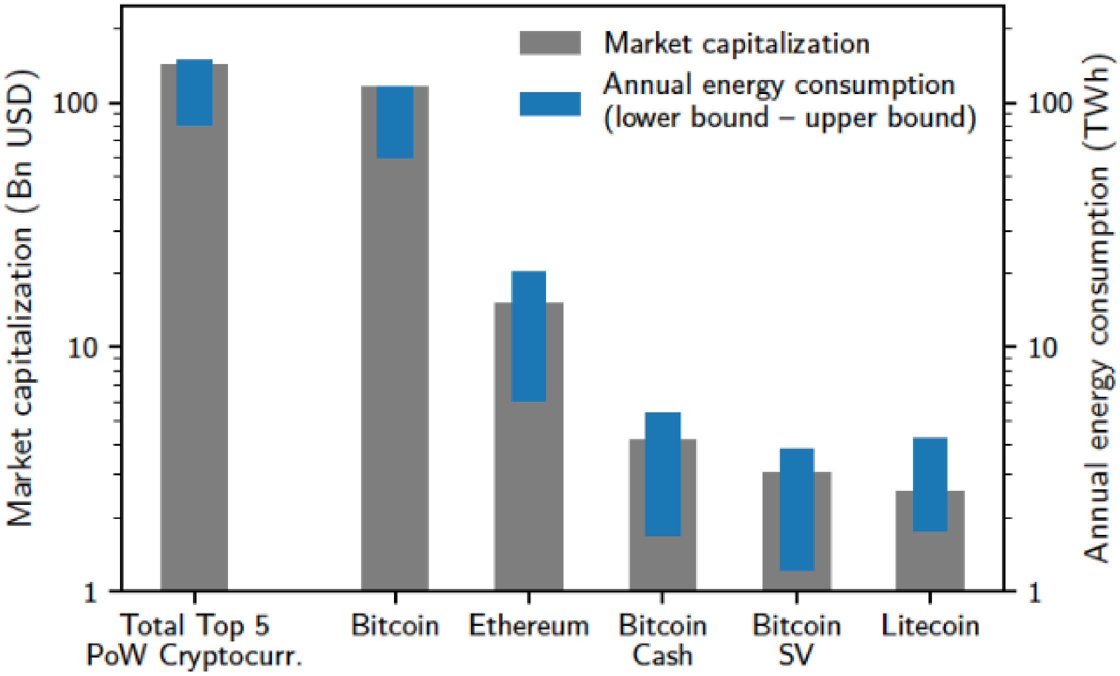
COMPARISON OF ENERGY CONSUMPTION

Several components contribute to the energy consumption of blockchains in general. They can be divided into three main categories: the consumption deriving from consensus mechanisms, the redundant computation and storage associated with the blockchain's operations, and the idle energy consumption of each node. In this section, we argue that while the consensus mechanism bears the lion's share of the responsibility for PoW blockchains' energy consumption, for non-PoW blockchains, nodes' idle consumption and redundant processing of transactions represent the main share of energy consumption. Two immediate implications of this result are that, contrary to common opinion,

- **PoW blockchains' energy consumption does not grow significantly when the number of transactions or the complexity of operations (like smart contracts) increases**, and that

- **non-PoW blockchains' energy consumption is so significantly smaller than that of non-PoW and in particular PoS and permissioned blockchains that it is questionable whether discussing the nuanced differences in their energy consumption is useful at all**.

Due to the nature of permissionless blockchains, certain variables required for accurately estimating the energy consumption of PoW blockchains, such as the number of miners and the hardware specifications of each miner, cannot be measured easily. For the contribution of consensus, researchers must rely on approximations to provide lower and upper bounds on energy consumption. Nonetheless, reasonable estimates are available based on the work of Vranken (2017), Krause and Tolaymat (2018), De Vries (2018), and others. An important factor that influences the energy consumption of PoW-based blockchains is whether the network permits highly specialised mining equipment or just general-purpose hardware. More specifically, a lower bound on energy consumption can be determined through the observable hash rate (the complexity of the computational puzzle is public, and so is the number of solutions presented in the form of new blocks, so the expected compute power can be derived easily) and the most energy-efficient mining hardware on the market. On the other hand, an upper bound can be determined via the assumption that mining is profitable, so the costs for electricity and hardware (and, in particular, electricity costs alone) do not exceed the accumulated block rewards and transaction fees. Hence, the upper bound depends on the price of the cryptocurrency, the number of new coins created per block, transaction fees, and the lowest electricity costs on the market. Taking these factors into consideration, Sedlmeir et al. (2020a) estimated that in early 2020, the energy consumption of consensus in Bitcoin ranged between 60 TWh and 125 TWh per year, and provided estimates on the energy consumption of the five highest valued (by market capitalisation) PoW cryptocurrencies, as illustrated in figure 1. Since the upper bound depends largely on the value of the cryptocurrency (for example, transaction fees represent only around 10 % of miner's rewards in Bitcoin), considering the substantial increase in the value of several cryptocurrencies in recent months indicates that the upper bounds of these estimates have increased substantially. This brings the upper boundary of Bitcoin's electricity usage likely to be higher than that of nations like Norway and Argentina. A detailed analysis also suggests that Bitcoin's energy consumption dominates the energy consumption of all other PoW cryptocurrencies combined: In their study, Gallersdörfer et al. (2020) estimated that Bitcoin accounts for approximately 2/3 of the consumption generated by all PoW blockchains.



Market capitalisation and the computed bounds on energy consumption for the 5 highest valued Proof-of-Work cryptocurrencies in early 2020. Note the logarithmic scale on the y-axis
Source: (Sedlmeir et al., 2020a)

As a consequence, while criticism of PoW's energy consumption is arguably justified, predictions that suggest that the energy consumption will massively increase further in the future obtained by interpolating the energy consumption to the expected number of transactions, as, for instance, conducted by (Mora et al., 2018), should not be taken seriously (Lei et al., 2021). The biggest threat of increasing energy consumption is a further considerable increase in the Bitcoin price, an increase in transaction fees, or a decrease in electricity prices (which is, however, unlikely to happen, considering the increased demand for electricity; and in times where electricity is very cheap, it may be renewable and spare anyway).

When it comes to PoS, CFT, and BFT based blockchains, the consensus mechanism consumes orders of magnitude less energy than PoW because there is no mining process. The range is typically specified by a 99.95 %, 99.98 % or even higher reduction in energy consumption (Beekhuizen, 2021) – comparable to the at least 99.98 % that PoW is responsible for Bitcoin's electricity consumption. The details depend considerably on the number of nodes and the hardware specifications for the blockchain under consideration. In BFT-based mechanisms that are often used in consortia, consensus' complexity increases super-linearly with the number of nodes, which implies increasing amounts of energy as more nodes participate. However, their energy consumption remains very limited for practical network sizes. In the end, in contrast to specialised mining hardware with high power consumption used in high numbers in PoW, CFT and BFT blockchains are usually running on commodity servers with an electricity consumption in the higher two-digit or lower three-digit range. As a result, a permissioned blockchain with 20 nodes will not consume significantly more than a few kW of electrical power when it is running (which is no more than the power consumption of charging a single electric vehicle), compared to a double-digit number of GW for Bitcoin, which is more than a million times more.

Additionally, one could argue that Bitcoin currently operates a single-digit number of transactions per second while a permissioned blockchain can operate hundreds to thousands of transactions per second. However, as mentioned, energy per transaction is not always a good metric, and proponents of Bitcoin rightfully claim that the transactions that happen on the Lightning Network (Poon and Dryja, 2016) could scale to thousands or even millions of transactions per second, which, as argued above, would not imply a considerable increase in energy consumption.

In permissionless blockchains using non-PoW-based consensus mechanisms and in permissioned networks that do not operate consistently at high load, the major share of energy usage derives from idle power consumption and, typically to a lesser extent, from the network's redundant operations. Because of this, energy consumption per transaction again provides inaccurate estimates also for these blockchains, as idle consumption remains unaffected by the number of transactions. As a general guideline, a blockchain network with N nodes based on non-PoW consensus mechanisms consume approximately N times the energy of a centralised system using hardware similar to that of the nodes (without taking into consideration potential backups on the one side and a larger number of cryptographic operations on the other side). However, it is practically impossible to estimate the idle consumption of nodes as users, particularly in public blockchains, tend to use a wide variety of hardware consuming various amounts of energy, and the differences between a desktop computer that runs only for a blockchain node (consuming on the order of 50 W) and a raspberry pi or a cloud instance that only consume on the order of 5 W or less is significant. For this reason, we place emphasis on the consumption coming from the blockchain's redundant operations, which dominates the estimate as soon as the hardware is tailored to the requirements of a node. However, to date, a large number of blockchain nodes likely has much higher hardware specifications than would be required, also because they want to be prepared for potentially increasing requirements in the future.

Two factors influence the energy consumption associated with redundant operations: the number of nodes performing specific operations concerning the consensus mechanism and the complexity of the workload (Sedlmeir et al., 2020a). Over the years, multiple methods have been developed to reduce the energy consumption of these two factors. For example, blockchains can employ sharding to reduce the consumption coming from the number of nodes that must perform the operations, i.e., reducing the degree of redundancy. Using sharding, a blockchain divides the nodes into subsets, and the transactions are verified only in one of these subsets, spending only a fraction of the recourses. Implementing sharding is heavily consensus-specific and can be challenging in blockchains using PoW but is rather straightforward in PoS. However, since fewer nodes validate the transactions, sharding makes a system more centralised and, thus, less secure. Hence, sharding can help balance the need for redundancy and efficiency but allows only for a bounded factor of improvement.

On the other hand, reducing the energy consumption associated with the verification of new blocks and the transactions included, specifically if operations are computationally intensive (for instance, a large matrix multiplication), can be achieved using succinct proofs, the most prominent representative of which may be Zero-Knowledge-Proofs (ZKP) (Canetti and Garay, 2013). These methods can utilise that instead of having all nodes re-compute the operation, a single party performs the computation more intricately and generates a proof for the correctness of the computation that is much less complex to verify than re-compute the original operation. The necessary calculations are hence carried out off-chain with just the computationally light verification taking place on-chain. When the number of nodes is large, the cumulative energy savings for the verifiers (i.e., all nodes) significantly outweigh the additional energy consumed by the “prover” (i.e., the client that computes the proof and sends it to a node in the form of a transaction). Consequently, this approach can help save energy. However, it should be noted that since energy consumption is in non-PoW blockchains, the major interest in these possibilities is because they are beneficial from a privacy and performance perspective, which is arguably the main reason for using ZKPs on blockchains).

Most public blockchains can run on low-end hardware today, like a raspberry pi, which consumes less than 5 W per device. Given that VISA and PayPal consume approximately 5,400 J (Visa, 2019) respectively 73,000

J (PayPal, 2020) per transaction when the companies' overall consumption is considered (in the case of Visa, data centres account for around 50 % of energy consumption), a non-PoW blockchain with low-end hardware could consume as much energy as VISA while operating around 1,000 nodes, and 15,000 nodes in the case of PayPal (which is more nodes than the 13,000 in the Bitcoin network, which is probably the blockchain with the most full nodes today). Consequently, medium-sized blockchains that run on reasonable hardware are comparable in energy consumption on a per-transaction basis, and with the stated optimisations, large permissionless blockchains like Ethereum will – once they run on PoS – likely not consume considerably more energy than today's centralised payment systems. Permissioned blockchains, on the other hand, only have a low degree of redundancy and – despite being more energy-intensive than a centralised server – still have an energy consumption comparable to common software applications and will most likely generate energy savings rather than additional consumption when new workflows can be digitised.

ENERGY CONSUMPTION OF THE ENERGY WEB BLOCKCHAIN

Energy Web (EW) is a global nonprofit organisation accelerating a low-carbon, customer-centric electricity system by unleashing the potential of open-source, decentralised technologies. EW focuses on building core infrastructure and shared technology, speeding the adoption of commercial solutions, and fostering a community of practice.

In 2019 EW launched the Energy Web Chain (EW Chain), the world's first open-source, enterprise-grade blockchain platform designed for the energy sector's regulatory, operational, and market needs. Since its launch, it has become the industry's leading choice as the foundational digital infrastructure on which to build and run blockchain-based decentralised applications (dApps). With a virtual machine identical to public Ethereum, developers can begin writing smart contracts and dApps for EW Chain with little to no additional learning curve.

The EW Chain boasts high scalability, low transaction costs, and lean energy consumption, thanks to its unique consensus mechanism. In contrast to Proof-of-Work (PoW) blockchains such as Bitcoin and Ethereum that rely on anonymous miners to operate the network via energy-intensive crypto mining, EW Chain uses a permissioned Proof-of-Authority (PoA) consensus mechanism in which a pool of known and trusted computers—called validator nodes—are responsible for validating transactions and creating blocks. The EW Chain's PoA consensus mechanism consumes a staggering six orders of magnitude less energy than Ethereum, while offering certain security, regulatory transparency, and considerable capacity benefits over Ethereum.

EW CHAIN'S ENERGY FOOTPRINT

A blockchain network like EW Chain or Ethereum is akin to a single computer that is replicated across many individual computers across the internet. Decentralised blockchain computers need a consensus mechanism - or a method by which a temporary "leader" is chosen to make decisions for the whole network for a short period of time. Consensus mechanisms can be competitive and energy-intensive like Ethereum's PoW method, or highly orderly and energy-efficient, like EW Chain's PoA method where "authority" validator nodes take turns proposing blocks to add to the chain in a round-robin fashion. By contrast, the most common alternative to PoA consensus, PoW, involves computers racing to solve arbitrarily difficult math problems - using vast amounts of computing power and energy in the process. Stripping away the competitive "mining" aspect from a blockchain drastically reduces its energy consumption. In fact, the energy footprint of a single *non-mining* blockchain node is comparable to a typical desktop computer.

A blockchain's energy footprint is the sum of the individual footprints of all of its miners or validator nodes - at present EW Chain has about 50 validator nodes across the globe. We estimate that each node consumes between 50 and 150 Watts of power at all times, depending on its components and HVAC cooling requirements. Taking the top end of this estimate, EW Chain's instantaneous power draw is about 7.5 kilowatts. In comparison, Ethereum draws roughly 1,000,000 times more power and Bitcoin consumes roughly 2.2 million times more power than EW Chain.

Measurements of EW Chain nodes over time suggest that power consumption is relatively constant, regardless of whether the blockchain is under heavy or light load. Power requirements may slowly grow over time as the blockchain "state" (the total stored smart contracts and account data) grows, more validators join the network, and transactions become more computationally intensive. But for now, it is safe to treat EW Chain's energy consumption as a constant.

AN ENERGY DAPP'S FOOTPRINT

Since the EW Chain is essentially a decentralised computer purpose-built for the energy sector, it has resource constraints like any other computer. When you evaluate one of the many decentralised apps (dApps) running on the EW Chain, you can easily calculate how much of the blockchain's resources it consumes and hence, its share of EW Chain's energy footprint. Things get interesting when you explore the impact design decisions have on the amount of blockchain resources a dApp needs to consume to deliver value to the energy sector.

For instance, a dApp designed to track thousands of home batteries participating in grid services might do the vast majority of its data processing activities off-chain and only make a total of four on-chain transactions per hour; whereas another application for a *single home* could be designed to do its data processing on-chain and use the chain significantly more than the dApp supporting thousands of homes. Not all energy dApps are designed with the same constraints or considerations in mind, and some applications that leverage digital identifiers (DIDs) anchored on the EW Chain could use the chain only *once per year* or less, yet still enjoy many of the security, authentication, and transparency benefits the EW Chain has to offer. Hence, it might be better to evaluate how much *value* a dApp derives from its share of the EW Chain's resources rather than how much energy it consumes. With proper use of DIDs and the surrounding suite of EW Utility Layer Services, the EW Chain could support 100's of millions of devices and applications.

HASHNET BLOCKCHAIN - OVERCOMING SCALABILITY AND PERFORMANCE BARRIERS

HashNET platform is focused on providing a new type of scalable, fast, secure, and fair decentralised solution, leveraging Distributed Ledger Technology (DLT) and consensus algorithm which keeps all positive characteristics of blockchain technology (decentralised, transparent, pseudo-anonymous) while significantly increasing transaction throughputs. HashNET uses an Improved Redundancy Reduced Gossip (Improved RRG) and "Virtual Voting" protocol for information transfer on a suitably designed network, which make it possible to achieve considerably lower traffic load than conventional push-based gossip protocols and traditional push-pull gossip. And it is the consensus mechanism that ultimately determines the level of security, speed of transactions and scalability of a network, making it possible to increase the number of transactions executed in second for more than 50 times, keeping the time to finality up to three times lower compared to existing, tested solutions (at the level of 3 to 8 seconds).

Scalability turns out to be often mentioned as one of the biggest challenges related to the wide-spread usage of blockchain technology. HashNET was built to support up to 50,000 transactions per second on layer 1 and is able to support millions of transactions per second on layer 2 (when form of sidechains applied). Even with hundreds of nodes, HashNET network is able to process all transactions in a matter of seconds, since the Improved RRG and "Virtual Voting" mechanism innovation eliminates inefficiency imposed by other based blockchain solutions.

Various efforts have been made by the development team to move scalability solutions to a second layer, to mentioned sidechains. Usage of the sidechain ensures that user interactions are shifted from the blockchain layer (1) onto a second layer (2), while guaranteeing risk-free P2P transactions between participants. Sidechains are separate blockchain networks, compatible with the mainchain. Sidechains have their own consensus mechanism, their own level of security, and their own tokens. Throughput of the blockchain would be a cumulative value of main and sidechain, thus creating enormous scalability potential of HashNET technology. It's also important to emphasise that if the security of a sidechain network is compromised, the damage will not affect the mainchain or other sidechains. Both networks are linked to each other via a "two-way peg" and can transfer any state. This way, tokens can be exchanged at a predetermined rate between the mainchain and the sidechain. The mainchain guarantees overall security and dispute resolution, and the transactions that are outsourced to the sidechain – although the mainchain contains the information on each event alongside timestamp and transaction signature information.

To take a look in depth, how the described scalability is achieved, is important to describe HashNET consensus mechanism. Each node in the network keeps a representation of the HashNET in its memory. The HashNET that each node has can differ, but through the process of gossip, the yet unknown events to the node are added to its HashNET representation. Next, we need to introduce the term of an event object as a data structure created by some node and containing the two hashes of the preceding events – parent event created by the same node ("self-parent") and the parent event created by some other node ("other-parent"). The node that is the creator of the transaction also puts a timestamp to the event object at the creation time, and the event is thus digitally signed. Each event object can optionally contain zero or more transactions making the event a container for those transactions. When the event gets gossiped the signature is sent along with it. Events can have zero transactions either when a node receives a sync event (HashNET difference) or when the node has just been spawned, thus creating the first event with no self-parent and no other-parent, and there are no pending transactions that this node is aware of in its transaction pool.

The goal of the HashNET algorithm is for nodes in the network to come to a consensus. The consensus is defined as agreement on the order of events. Furthermore, by agreeing on the timestamps for each event, the order and timestamps for each transaction are determined as well. Nodes can call each other at random for syncing and determining which events they don't have recorded yet in their instance of the graph.

Since a green energy transition has been a central pillar of EU policy-making, it is necessary to adapt energy infrastructure to the future needs of the energy system, within decentralised network. It is clear that if building blockchain applications move toward less energy-intensive methods of verification, there should be a resultant decrease in blockchain energy consumption. It does not require miners to create a chain of blocks to record transactions, and thus, an enormous amount of energy is saved.

While Redundancy Reduced Gossip (RRG) and other asynchronous distributed consensus protocols provide communicational and computational efficiencies, additional implementation improvements are necessary to handle large fast-growing systems. A direct implementation of such protocols could require exchanging as much as O(n^3) messages for reaching a consensus on a single binary outcome, which would make them not practical and unsustainable for systems where the number of nodes, n, is large. Thus, the imperative of HashNET development strategy was to implement the consensus protocol in a way that minimises communicational load due to information transfer among nodes. It leverages the fact that every node has sufficient information on the entire HashNET structure, including information about events and their propagation through the network to compute content of the vast majority of messages required by Improved Redundancy Reduced Gossip (IRRG) protocol, thereby eliminating the need for sending them and consequently, significantly reducing communication requirements. A somewhat similar approach towards reducing communication requirements in an implementation of a different consensus protocol has been proposed before, but unlike the HashNET system, a critical requirement imposed by each was that the number of nodes is constant and must remain fixed constant throughout. An important prerequisite for efficient computation of consensus is that the total number of nodes (“voters”) needs to be known. HashNET overcomes this difficulty by assigning to every node the vote weight that is equal to their stake at a given point of time. By assigning node weight to be its stake in the network, HashNET achieves the ability to calculate votes instead of waiting for and/or sending actual votes over the network. As long as two-thirds of the nodes are safe, consistency of consensus can be ensured, while in the worst scenario of cyber-attack of more than one-third of the nods in the network, all history of transaction remains unchanged and can be replicated. All the servers at the same time would need to be destroyed to erase the history.

For high volume and velocity of the transaction, the additional note has to be made - HashNET poses specific functionality of ordering transaction, allowing fair execution. If the main chain (layer 1) alongside sidechains installed to handle millions of transactions proves not to be enough in peeks of, let us say, IoT based large number of applications, the HashNET will adjust to the terms. Additionally, if keeping it on layer 1, it poses a property of creating the (optimised size) bulks of transaction proposals, HashNET would make fair ordering action, imposing the 'first in – first out' method on transaction requests. The validation phase would be executed for each bulk of transaction request, again imposing same the 'first in – first out' method to ensure fairness. Hereby is important to emphasise that the method of adding a sidechain and creating a batch of transaction bulks are not mutually exclusive and they add up to solution scalability. It's the matter of the use case the blockchain is used for how many if any sidechain needs to be used or batching option is efferent enough.

HashNET key blockchain infrastructure capabilities:

1. Ensures completion of 50.000 transactions per second on layer 1,
2. High latency since the time to finality is 3 to maximum 7 seconds

   and both achieved just on layer 1,

3. The solution can support millions of transactions per second introducing layer 2, as additional sidechains.

Hashnet reaches high scalability with a limited increase of the energy demand without compromising on security. The consensus mechanism used in HashNET requires minimum electrical consumption while the way transactions are recorded needs minimum storage space. Efficiency-wise, the HashNET protocol eliminates many obstacles. The communication for consensus in the network is very energy-efficient, since information exchange is kept at a minimum, thereby needing no computing power. The gossip protocol allows sending a lot of information quickly through the network at low computing power input, making it even more suitable for energy-efficient applications. Unlike other consensuses that require every node to receive an updated graph that tend to lead to performance inefficiency with an increasing number of nodes, HashNETs' Improved Redundancy Reduced Gossip (Improved RRG) protocol achieves considerably lower traffic load than conventional push-based gossip protocols and conventional push-pull gossip protocols while maintaining the same probability of successful delivery. When the event gets gossiped, the signature is sent along with it. Events can have zero transactions either when a node receives a sync event (HashNET difference) or when the node has just been spawned, thus creating the first event with no self-parent and no other-parent, and there are no pending transactions that this node is aware of in its transaction pool. This eliminates potential performance inefficiency the blockchain can face with an increasing number of nodes.

Section 2: Blockchain Energy Consumption Indices

OVERVIEW OF VARIOUS METHODOLOGIES

It's a challenging task to accurately quantify the electricity consumption of the Bitcoin network, and what one finds across methodologies is that it's largely an oversimplification based on several educated assumptions. Overall, it's an iterative ongoing process of adding more pools and extrapolating more accurate data to be able to accurately estimate the global electricity consumption and ultimately the carbon footprint of Bitcoin. It should be mentioned that solid methodologies for the estimation of the energy consumption of blockchain technologies are only available for the PoW, therefore the energy efficiency analysis is mainly focused on the Bitcoin blockchain.

Often, however, the significance lies in providing a basis to reason with the terawatt-hours (TWh) consumed rather than to only quantify this metric. Reasoning comes by asking questions such as whether the electricity consumed is worth the utility which Bitcoin provides, but this too is a flawed approach. Although Bitcoin may consume a relatively significant amount of energy, the right question to ask perhaps draws back to whether the electricity produced is from renewable or non-renewable sources. Or to take this one step further, challenge the entirety of non-renewable energy production rather than speculate on what consumes it. What's clear is that there remain two diametrically opposed viewpoints on Bitcoin's environmental mining footprint, both of which (often incorrectly) use various data points to support their own narratives.

In September 2020, Cambridge Centre for Alternative Finance (CCAF) published research showing that although 76% of hashers report using renewables as part of their energy mix, non-renewables still represent 39% of the total hashing energy consumption (Blandin et al., 3rd Global Cryptoasset Benchmarking Study - CCAF publication 2020). Bitcoin hashers' preference for renewable energy sources is perhaps relatively higher than other electricity uses, the reason being that Bitcoin miners often identify remote inaccessible locations that are not connected to the grid. This is common practice to maximise revenue margins. Here, miners can reap the benefits of cheaper renewable electricity which may be produced in surplus and cannot be used, transported or efficiently stored, for example, surplus hydro, solar, and wind power production. (CBECI 2019)

Various methodologies have been implemented in recent times to estimate the electricity being consumed. The two variables (Bitcoin price and mining hashrate) are volatile metrics and so it makes sense for these indices to track real-time data rather than use more distributed periodic snapshots. The two most widely referenced real-time models are the Cambridge Bitcoin Electricity Consumption Index (CBECI) and the Digiconomist Bitcoin Energy Consumption Index. Both methodologies use interesting economic models, based on certain assumptions.

Contrasting these two methodologies from a high level; CBECI implements a bottom-up techno-economic approach by looking at the actual mining equipment to build a model based on the hardware being used at a specific time and then using the efficiencies or specs of that mining equipment to extrapolate the annualised Bitcoin electricity consumption. (CBECI 2019)

Whereas the Digiconomist index, created by Alex de Vries, implements an economic top-down approach by estimating Bitcoin miner revenues and then using an assumption that a portion of that revenue is used to pay for electricity. By modeling an average electricity cost globally, the Digiconomist index can then calculate the energy being used. (de Fries, Digiconomist, Bitcoin Energy Consumption Index)

Neither of these methodologies (CBECI or Digiconomist) is seen as incorrect and in research it is always useful to have diverse approaches to provide multiple perspectives to a single question. As these methodologies develop in the future and more reliable data becomes available on both ends, the delta between their respective underlying assumptions would ideally get smaller.

THE CAMBRIDGE BITCOIN ELECTRICITY CONSUMPTION INDEX (CBECI)

The Cambridge Bitcoin Electricity Consumption Index mentioned herein, was developed, and launched in July 2019 by the Cambridge Centre for Alternative Finance; a research institute of Cambridge University based in Judge Business School.

The CBECI aims to provide real-time estimates of the total electricity consumed by the Bitcoin Network while also providing live comparisons of alternate electricity uses, thus putting the annualised terawatt-hours (TWh) into perspective.

CBECI provides neutral and independent data visualisations and interpretations for researchers, regulators, policy makers, the media, and others, highlighting the non-biased facts. The extrapolation of estimated electricity consumption is derived by charting a theoretical lower bound and upper bound of Bitcoins electricity consumption at any time. The theoretical lower bound assumes every Bitcoin miner is using the most efficient commercial mining equipment; whereas equally unrealistically the theoretical upper bound assumes that every miner is using the least efficient, but still profitable equipment at the time (CBECI 2019). As the price of Bitcoin increases more equipment potentially becomes profitable and as a result this equipment comes online and the network hashrate increases.

The actual Bitcoin electricity consumption estimate sits somewhere between the theoretical upper and lower bound and is calculated using a real-time weighted average of a basket of hardware that is included based on equipment specs (CBECI 2019). Interestingly, the divergence between the theoretical upper and lower bound increases over time as BTC price spikes. Today the upper bound is ten times the lower bound, whereas in 2018 it was only about three times.

CBECI also displays a Mining Map (either global or China-focused), which visualises the approximate geographic distribution of Bitcoin hashrate. The average hashrate share by country is also available for display in monthly intervals starting from September 2019.

EXISTING/FUTURE EXTENSIONS OF THE METHODOLOGIES TO CALCULATE ELECTRICITY CONSUMPTION OF OTHER BLOCKCHAINS.

As Bitcoin mining data becomes more accessible, democratised and reliable, we expect electricity consumption estimates to become more accurate and precise. This includes the overall distribution of data being collected. Currently, there is a bias of data mainly from China, as this is predominantly where Bitcoin miners are located. Not all mining pools are willing to share data. For example, CBECI currently collects data from 3 of the largest pools (Poolin, BTC.com and ViaBTC). This represents on average 37% of the global hashrate for the displayed period (2019.09-2020.04) and is skewed toward China (CBECI 2019). Ultimately, the next phase of CBECI, once reliable geographical data is obtained, is to estimate the global carbon footprint of Bitcoin mining.

Over time the Cambridge Centre for Alternative Finance plans to increase the Bitcoin mining sample size, update the mining map, update and add more comparisons, (for example, comparison to gold production is currently being worked on. This is a daunting task since data disclosure is mostly vague and unreliable from mining stakeholders. Not to mention that the gold mining industry relies on multiple subcontractors within the supply chain to get the gold from extraction to market. Even the energy consumption for transportation of gold is significantly energy-intensive. Other complexities include reliance on diesel generators where consumption data is often unclear (Peyravi & Girard, CCAF).

Ethereum mining is more diverse than Bitcoin mining which is evidently more industrially scaled. The reason being that Ethereum mining is an area dominated more so by a larger variety of retail players, using a wider range of available equipment, with the price they pay for electricity varying anywhere between $0 (stolen electricity) to $0.20 per kilowatt-hour. This complicates and drastically increases the theoretical aforementioned divergence of a potential electricity consumption estimate, with a probable massive difference between CBECI's theoretical upper and lower bound estimates, when compared to Bitcoin (Dek, CCAF).

Ethereum, in particular, is an interesting example. In the short term, with Ethereum Improvement Proposal (EIP1559) expected to be included in the London hard fork sometime in July 2020, there is an evident divide on sentiment as developers support this fork, while many miners still oppose it believing they are less incentivised to include EIP1559 when it becomes available. In the longer term with Ethereum 2.0 planned to be rolled out, this represents a complete overhaul of the Ethereum consensus mechanism from the current proof of work (PoW) algorithm to a proof of stake (PoS) alternative. As becomes quite evident, any index to estimate Ethereum's electricity consumption is more volatile, less accurate and ultimately only temporary until PoS is implemented. Digiconomist currently displays a beta index of Ethereum Energy Consumption (de Fries, Ethereum Energy Consumption Index), while the Cambridge Centre for Alternative Finance also plans to explore implementing an Ethereum Electricity Consumption Index, using the unique bottom-up techno-economic approach (Dek, CCAF).

On a more experimental note, research is being done to identify the proportion of mining chips connected to the network (Helmy, 2020). By plotting the winning nonce value against block height (or time) often unique patterns emerge. The cause of these patterns varies across networks and, generally, they have been associated with either pool, software or hardware activity. If the pattern is caused by hardware one can refine the assumption made by existing electricity estimates such as CBECI. This is an area of ongoing research. (Eisermann, CCAF).

It is evident that this is an ongoing process of iterative progress, and across all methodologies it's a matter of refining research and gathering more reliable data. Electricity consumption indices today are representative of the current state of research and data available.

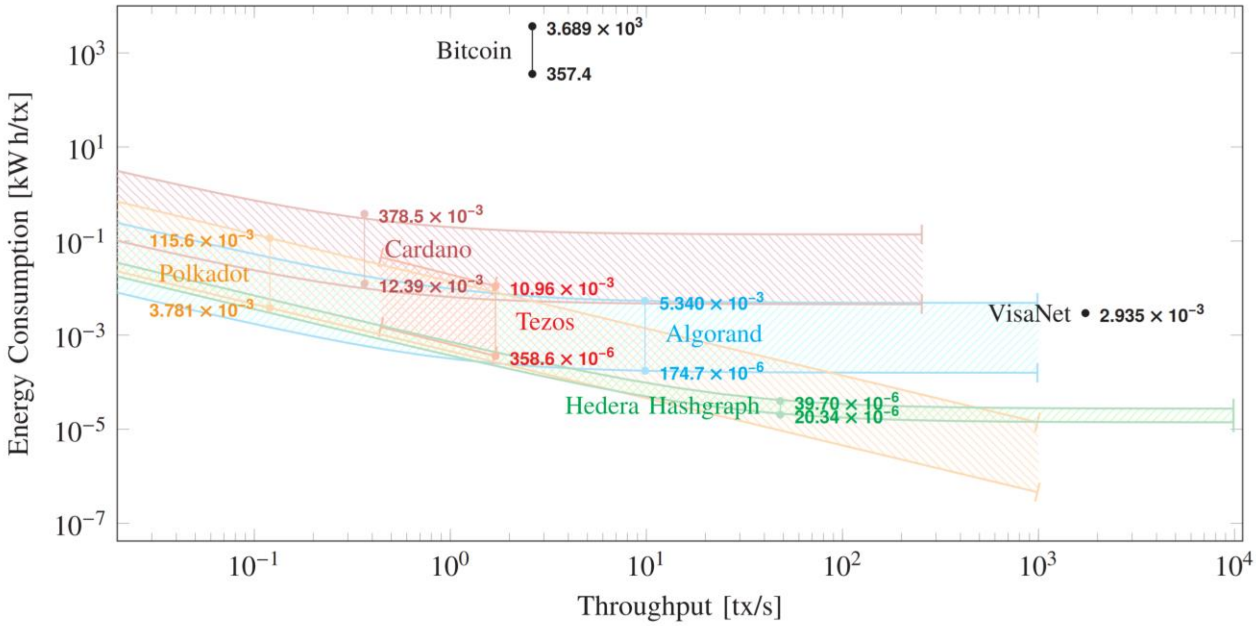
In conclusion, it should be mentioned that CBECI (bottom-up methodology) measures the specific hardware consumption of various mining hardware, using a published updated list of hardware specs. It then assumes that certain hardware is being used when the BTC price is at a level for that specific hardware model to be profitable. On the other hand, Digiconomist (top-down methodology), looks at miner revenues and makes certain financial assumptions again based on the BTC price at the time for that miner to be profitable. Extrapolating the expense part of miners (ie. primarily electricity consumption). One may observe that both methodologies are based on reason but rely on certain assumptions. The data set and the sample size is limited in all studies thus far, which is also the main limitation of both approaches. CBECI will be updating data sets in the short term as well as broadening participants who provide this valuable data, so we are not too concerned. Already existing data is already representative enough. CBECI is also in the process of extrapolating algorithms that would accurately estimate energy mix and carbon footprint of bitcoin mining.

EVALUATION OF ENERGY CONSUMPTION OF PROOF-OF-STAKE BLOCKCHAINS

In September 2021, the UCL Centre for Blockchain Technologies (UCL CBT) published a discussion paper that presents the results of the comparison of different Proof-of-Stake (PoS) blockchains, in order to validate the hypothesis that PoS consensus mechanism is more energy efficient compared to PoW-based blockchains. To perform this task, the UCL CBT team used a mathematical consumption model that predicts expected energy consumption per transaction, as a function of network load. The model was then applied to six different PoS-based DLT systems. The analysis confirmed that their energy consumption per transaction was at least three orders of magnitude lower than that of Bitcoin. Furthermore, UCL CBT discovered significant differences among the analysed PoS-based systems themselves.

The different PoS-based DLT systems under evaluation were:

- ALGORAND: Algorand uses a "pure-proof-of-stake" (PPoS) system where relay nodes store the entire ledger and non-relay nodes store up to approximately 1,000 blocks
- CARDANO: Cardano is the only "unspent transaction output" (UTXO)-based system in the comparison set. In Cardano, nodes store every transaction ever made.
- ETHEREUM 2.0: Ethereum is a commonly used blockchain undergoing its transition from proof-of-work (Ethereum 1.0) to proof-of-stake (Ethereum 2.0).
- HEDERA: In Hedera, “proof-of-stake” (PoS) is used to protect the network via a virtual-voting algorithm. Token holders stake Hedera’s native cryptocurrency to nodes, adding weight to a node’s voting power.
- POLKADOT: In Polkadot’s “nominated-proof-of-stake” (NPoS), each node delegates stake across 16 validators, among which the stake is divided equally.
- TEZOS: In Tezos’ “liquid-proof-of-stake” (LPoS) consensus mechanism, token holders delegate their validation rights to other token holders (called validators) without transferring ownership of their tokens.



Energy consumption comparison chart (Source: UCL Centre for Blockchain Technologies)

One of the important aspects of the modelling and subsequent analysis carried out by the UCL CBT team is the fact that the energy consumption of the different types of PoS blockchain heavily depends on the number of validator nodes participating in these systems. Therefore, permissioned blockchain networks tend to be characterised by lower energy consumption, compared to their permissionless counterparts, without meaning that permissioned blockchains are less energy-consuming. However, it should be pointed out that the decentralised nature of blockchain-based systems should not be sacrificed for lower energy consumption. As UCL CBT reports mentions, “[e]ven if a reducing effect of permissioning on energy consumption could be stated with certainty, this should not be misinterpreted as an argument for increased centralisation or an argument for permissioned networks over permissionless ones. This becomes obvious when considering a permissioned DLT system in extremis: such a system would consist of only a single validator node and would thus be effectively centralised.” Finally, for both permissioned and permissionless blockchain-based systems the selection of suitable validator hardware is central to energy consumption.

Section 3: Blockchain Performance

BLOCKCHAIN PERFORMANCE COMPARISON

Since 2009, numerous cryptocurrencies have been developed, however, Bitcoin is the largest and most popular representing over 60% of the total market of cryptocurrencies. The combined market capitalisation of all cryptocurrencies is approximately USD $1.72 trillion (as of March 2021). Other key currencies in this market are Ethereum, Cardano, Litecoin and Bitcoin Cash. However, it should be mentioned that the performance analysis carried out in this section is not only related to cryptocurrencies, but also to the other use cases that used the underlying blockchain technologies that correspond to these cryptocurrencies.

Top 5 Mineable Cryptocurrencies by Market Capitalisation on 03/08/2021

Name	Symbol	Algorithm	Market cap [USD bn]	Protocol
Bitcoin	BTC	SHA-256	1 044	PoW
Ethereum	ETH	Ethash	211	PoW
Cardano	ADA	Ouroborous	37	PoS
Litecoin	LTC	Scrypt	13	PoW
Bitcoin Cash	BCH	SHA-256	10	PoW

To understand the performance of these blockchains and to evaluate their energy consumption a number of key parameters should be analysed. Thus, Bitcoin, Ethereum, Litecoin, Cardano were compared based on the following indicators: block time, block size and number of transactions over the period of three years from October 2017 to March 2021 as all these values directly or indirectly affect the above-mentioned index.

Firstly, block size. Block size is a key metric since bigger blocks lead to heavier data storage costs. Moreover, when the block size approaches the maximum value problems may arise, such as a slowdown of the network and increasing transaction fees. Network utilisation is an important metric in understanding transaction fees – it can be used to understand how much demand there is for the available block space. Block space is scarce, in a Proof of Work blockchain such as Bitcoin the decision on which transaction to include are partially dependent on the transaction fee users are willing to pay. Miners are monetarily incentivised to include transactions that have the highest fees. Per the law of supply and demand, if the demand to include transactions in a block increases, but the supply is capped based on block size, then the determining factor will be the price users are willing to pay to have their transaction included. Through this, blockchain users start competing for the right to include their transaction in the block and pay increasingly higher fees to maintain priority. Moreover, this leads to the confirmation of other transactions taking more time.

Figure 1 depicts the average block size comparison among BTC, ETH, LTC, ADA and BCH in the period from 2017 to 2021.

Based on data, the size of Bitcoin blocks remained on average 1MB while the size of Ethereum and Litecoin blocks are almost 1000 times smaller and equal to 26178 bytes and 39002 bytes respectively. The average Bitcoin Cash block size is also high in comparison to other coins and equals to 165 Kilobyte or 0.165MB. As for Cardano, the average block size is around 1200 bytes. So, BTC transactions usually have a higher average fee as users are competing for the right to include their transactions in the block and pay increasingly higher fees to maintain priority. On the other hand, miners compete against each other for limited block rewards, and they are interested in joining miners' networks that leads to hashpower increasing (will be considered further). Moreover, the data storage costs are also higher.

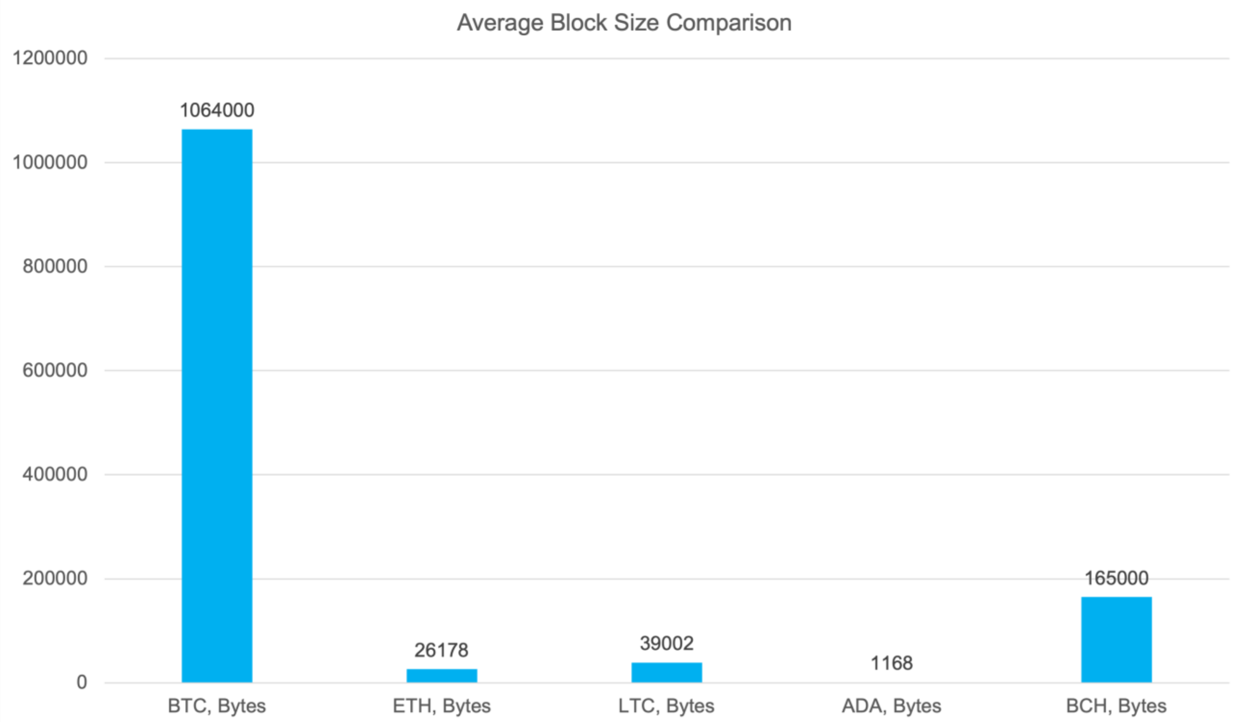


Figure 1: Average Block Size Comparison among Bitcoin, Ethereum , Litecoin, Cardano and Bitcoin Cash (2017-2021)

A second indicator to analyse is block time as this parameter directly affects the difficulty of mining. Based on data, Bitcoin takes almost 600 seconds on average to generate a block as well as Bitcoin Cash. A bit less time is taken by LTC and it is around 150 seconds or almost 3 minutes. On the other hand, Ethereum needs 14 seconds. As for ADA, historical data is not available, but average block time is about 40 seconds.

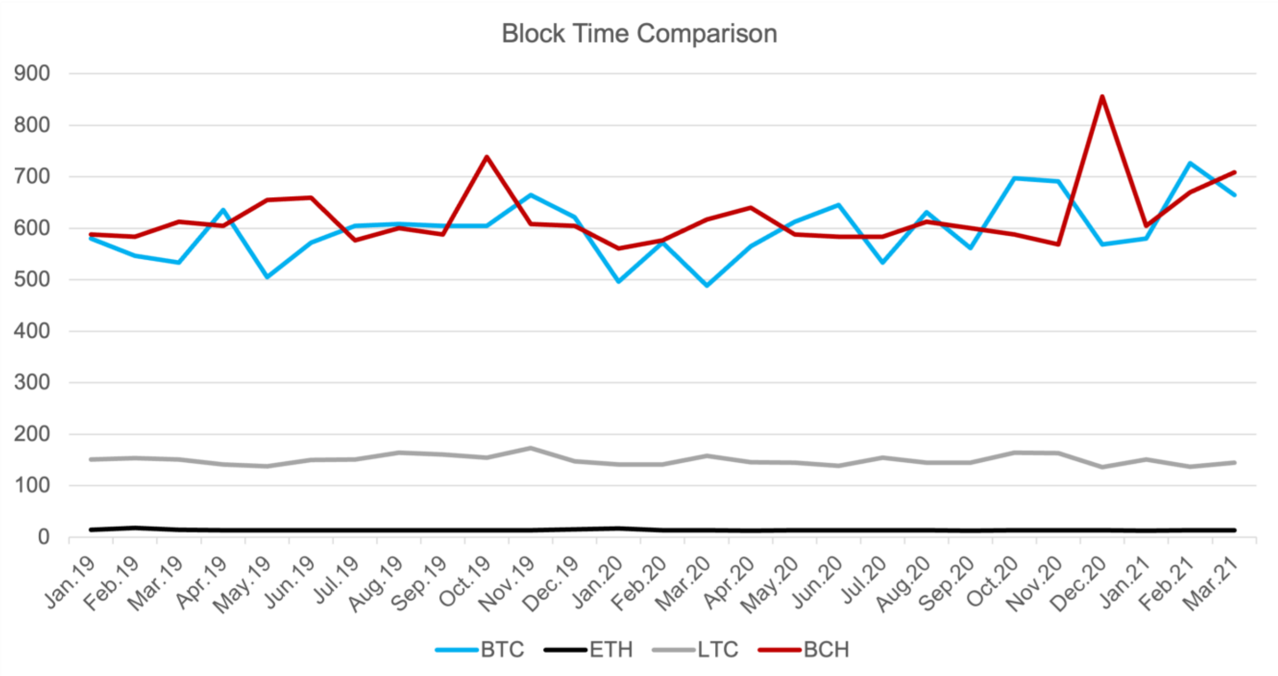


Figure 2: Average Block Time Comparison among Bitcoin, Ethereum, Litecoin and Bitcoin Cash

The third indicator important for understanding blockchain performance is the number of transactions. Figure 3 shows that transacting on the Ethereum network has become popular compared to other protocols. The popularity of Ethereum among investors from software developers, healthcare advisors, finance professionals, hardware producers, to mention a few, has rocketed upwards due to some of its unique characteristics. As it offers users access to several Decentralised Finance (Defi) projects, dApps, and smart contracts. For this reason, investors are increasingly moving capital into Ethereum – rather than simply using it for transactions the protocol has become the base layer for practical usage across different industries, including energy distribution, finance, medicine, art, and gaming.

The total number of ETH transactions reached almost 36,000 in February 2021. Regarding the average number of transactions per day and per second for the period from October 2017 to March 2021 they are as follows:

Blockchain name	Number of transactions	Average transactions per sec
Bitcoin	290,598	3.3
Ethereum	777,787	9
Litecoin	39,981	0.46
Cardano	5,678	0.07

Bitcoin Cash	52,646	0.6

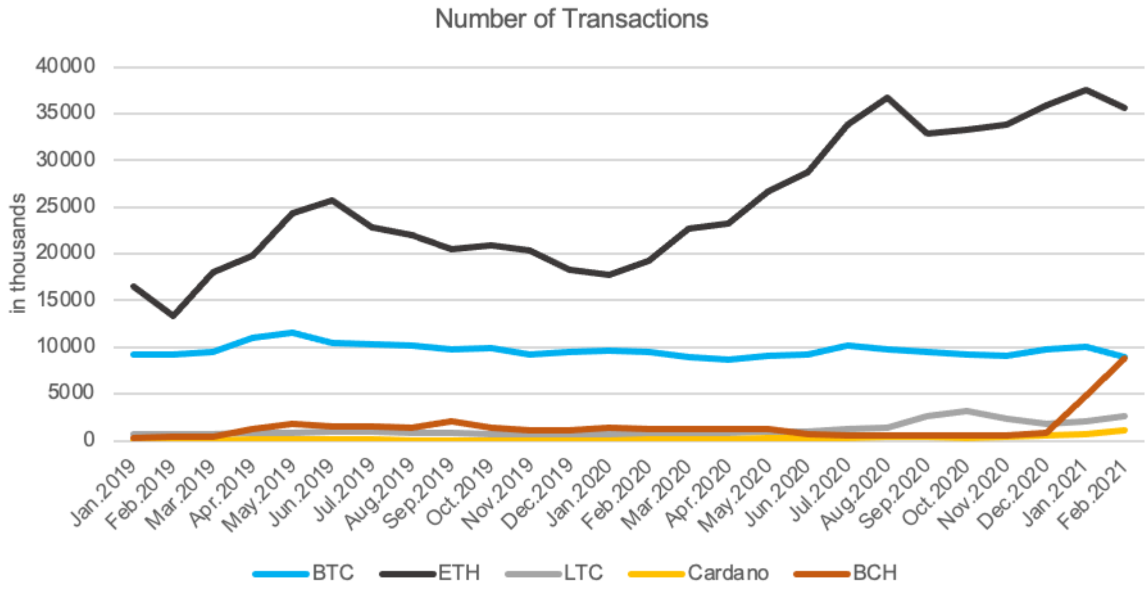


Figure 3: Number of Transactions Comparison among Bitcoin, Ethereum, Litecoin, Cardano and Bitcoin Cash

The final indicator to be covered is difficulty, or network difficulty. It is a value that indicates how hard is to find a hash below a given target, in other words, it is a parameter that shows the cost of finding one block in the cryptocurrency network. For better understanding, the notion of “hash rate” should be identified. The hash rate reflects corresponds to the total power of the mining equipment used in the cryptocurrency system and is displayed in hash/sec (H/s).

Thus, difficulty is a relative measure of the amount of resources required to mine coins which rise or fall based on the amount of computing power consumed by the network, known as its hashrate. The difficulty of mining is constantly growing to keep the target block time.

The designation H/s is not commonly used, it is orders of magnitude too small, and rates displayed in H/s would be a number with at least eighteen zeros. The following designations are mainly used: terahesh/sec (TH/s) and exahesh/sec (EH/s), where TH/s = 1,000,000,000,000 H/s, and EH/s = 1,000,000 TH/s.

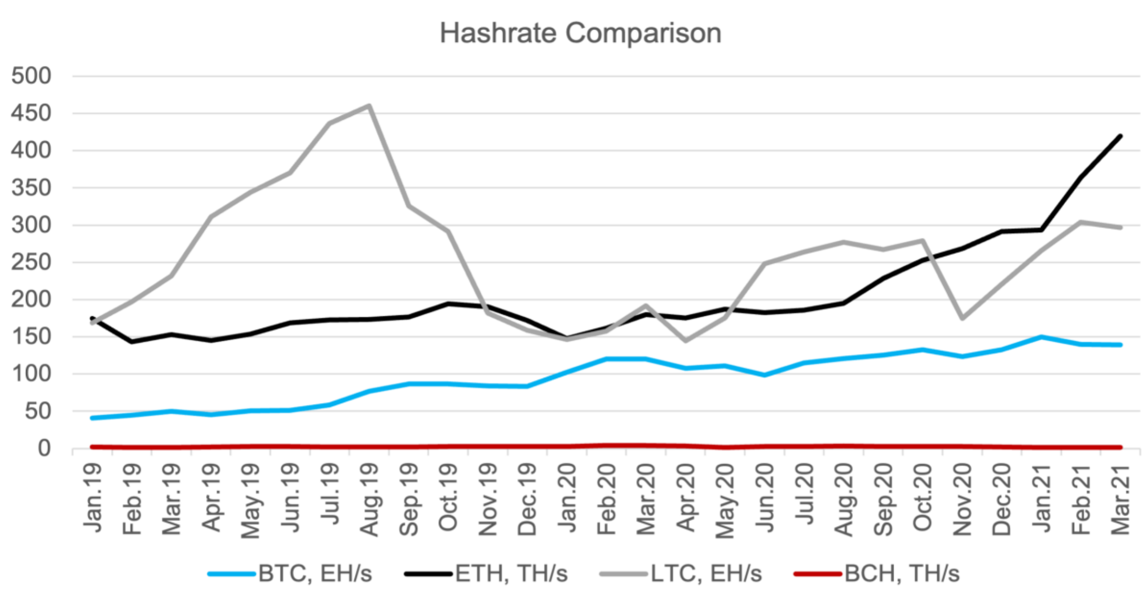


Figure 4: Difficulty Comparison among Bitcoin, Ethereum, Litecoin and Bitcoin Cash

As cryptocurrencies become more popular, the number of computers participating in the network increases. As it was mentioned above miners compete against each other for limited block rewards.

As more and more miners are attracted to mine bitcoin and reap financial rewards, the complexity to generate a new block accordingly increases – thereby reducing the rate at which new blocks are mined. The difficulty of mining in the Bitcoin network is adjusted automatically after 2,016 blocks have been mined. Adjusting the difficulty up or down depends on the number of participants in the mining network and their aggregate hash power. If new participants have joined the cryptocurrency mining, it means the hash rate has grown and more energy is consumed.

Figure 4 shows the difficulty of generating a new block among main cryptocurrencies. Bitcoin difficulty rose as high as 155 million TeraHash per second. The difficulty of mining a block in other blockchains is also growing, but Bitcoin remains the highest consumer of hashing power.

Furthermore, based on the figure below it is clear that Bitcoin and Ethereum energy consumption increase and reached the highest rates in March that are 78.04 TWh and 25.19 TWh, respectively. In addition, total carbon footprint for BTC transactions equals to 41 Mt CO2 yearly and 14 Mt CO2 for ETH transactions.

According to Digiconomist research, almost 792 kWh of electrical energy is consumed to proceed with one transaction in Bitcoin that equals to 376 kg CO2 of carbon footprint, which is the same as Bolivia’s average electrical energy consumption per capita. Concerning Ethereum, one single transaction takes 63 kWh of electrical energy or almost 30 kg CO2 of carbon footprint or Liberia’s average electrical energy consumption per capita. With the increasing popularity and usage of the Bitcoin blockchain, as well as the increased security requirements associated with the increased economic value of the cryptocurrency, the PoW system will lead to increasing demand for energy.

Based on [bitinfocharts.com data](), it is possible to calculate the amount of value transacted per CO2-emitted. The average BTC transaction value is 39,960 USD for the last year and 2,158 USD for ETH transactions. That means that 106 USD on the average in BTC transacted per 1 kg CO2-emitted or 71 USD in ETH.

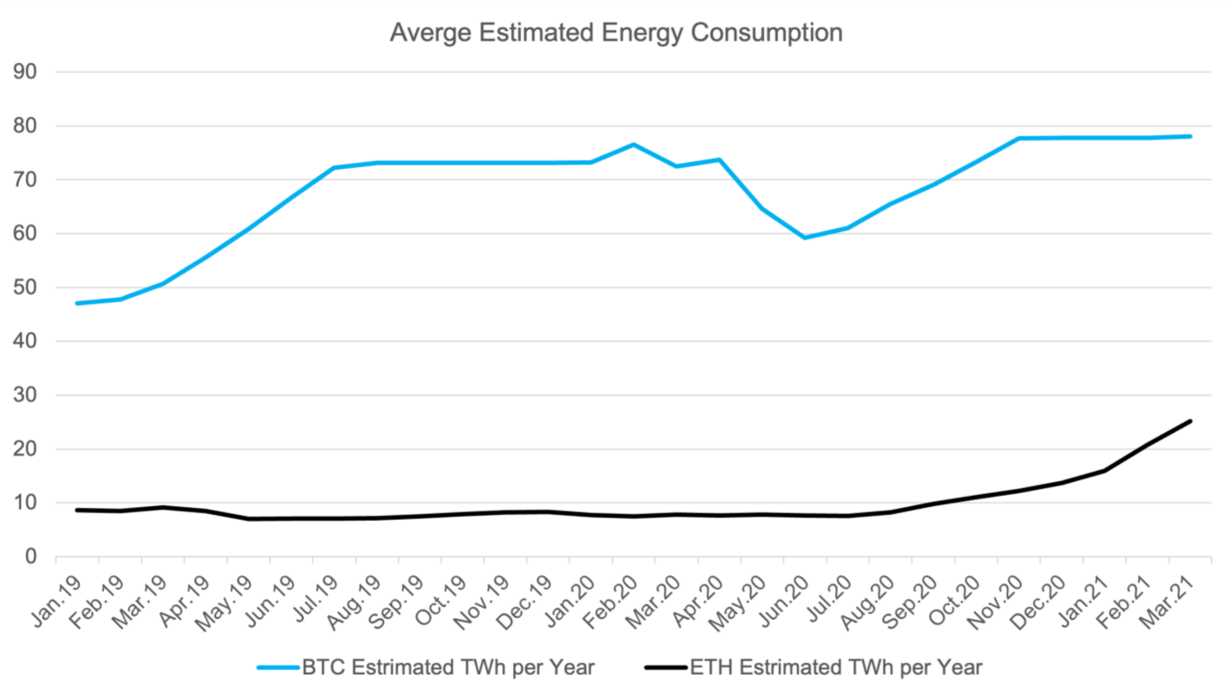


Figure 5: Bitcoin and Ethereum energy consumption worldwide

When it comes to blockchain performance there are clear advantages and disadvantages of each unique protocol and consensus mechanism, the main problem of Bitcoin is its scaling as it is restricted to a maximum number of transactions because of its block size. Each block, generated in around 10 minutes reaching 1MB which limits the transaction throughput to 2-4 transactions/sec. The average Bitcoin Cash block size is also high in comparison to other coins and equals to 165 Kilobyte or 0.165MB, however, its throughput is 0.6 transactions per second. Both, BTC and BCH have high difficulty levels and reached the highest rates in March. As for LTC and ADA, their average block size is 39,002 bytes and 1,200 bytes respectively, block time is 150 sec and 40 sec and throughput is constantly smaller just 0.46 LTC transactions per second and 0.07 ADA transactions per second.

ETH performance shows that it needs just 14 seconds to generate the block with an average size of 26,178 bytes, plus it is the most popular cryptocurrency based on the number of transactions with a throughput of 9 transactions per second. Hashrate for this currency is also growing and reached the indicator of 425 TH/s in March. Moreover, based on Digiconomist research, Bitcoin and Ethereum energy consumption increase and reached the highest rates also in March that are 78.04 TWh and 25.19 TWh, respectively.

COMPARISON OF CRYPTOCURRENCY MINING INFRASTRUCTURE

Rapid advances in technological innovation, including automation, digitisation, and electrification, are having a fundamental impact on the cryptocurrency mining sector.

The technology used by miners has advanced over time. Early miners were able to earn Bitcoin relatively easily with unspecialised equipment. On January 3rd, 2009, Satoshi Nakamoto created the first block of the Bitcoin Blockchain, hashing using the central processing unit (CPU) of his computer. However, as more units began to mine the network, the difficulty of the hashes they were trying to solve increased.

As interest in Bitcoin mining increased, miners discovered that graphics cards (GPUs) could more efficiently run hashing algorithms and aid in mining. These chipsets provided very fast processing power, more specialised in parallel computing when compared to CPUs. The world-leading GPU designers and manufacturers have been Nvidia and AMD (post the ATI acquisition in 2006), maintaining a global dominance in this market up to this day.

Field Programmable Gate Arrays (FPGAs) then replaced graphic cards, as the circuits in an FPGA could be configured and programmed by users after manufacturing. FPGAs are more expensive than CPUs and GPUs but they are also quite efficient in their use of electricity.

Finally, in 2013 fully customised Application Specific Integrated Circuit (ASIC) appeared and replaced these and graphic cards. ASICs are designed for a particular use such as Bitcoin mining.

The launch of Bitcoin ASICs spurred professionalisation of the mining industry. ASICs used to mine Bitcoin are usually housed in temperature-controlled data centres with access to inexpensive electricity.

Mining data centres are now industrial-scale facilities with management and servicing on par with traditional cloud data centres.

There are several factors that contribute to ideal mining locations and include energy costs, regulations, and technology. Often the energy costs are affected by geographical characteristics like proximity to hydroelectric or other renewable power or lower ambient temperature that reduces the need for cooling. Simultaneously, cooling energy, the power required to keep mining devices and mining farms cool, adds extra 30-50% on power consumption globally.

Historically, most large mining farms such as Poolin, F2Pool, etc., have set up their operations in China because of electricity cost and various available sources of electricity. As the People's Republic of China is sceptical about Bitcoin and other cryptocurrencies, mining operations are diversifying geographically with the cost of electricity being the main consideration. Local and national governments around the world have reacted differently to the rise of Bitcoin, with some are actively developing cryptocurrency industries, some are restricting cryptocurrencies, and some are regulating cryptocurrencies to balance financial innovation and risk management. Many countries offer competitive electricity rates, including Iceland, Canada, and the US.

It should be underlined that three main factors contribute to the energy consumption of cryptocurrency mining:

1. hardware computing power.
2. network hashrate or the difficulty.
3. the thermal regulation for the hardware.

The two most popular methods of mining BTC, ETH, LTC or BCH are ASIC and GPU mining.

Elwood research suggests that when comparing ASIC miners versus GPUs, the benefits are not as clear as there is a deliberate effort to keep the network running on easily accessible hardware rather than purpose-specific mining hardware. Nonetheless, ASICs have managed to outperform GPUs. Actually, the efficiency gains from ASICs could not be matched by any of the more general-purpose devices that preceded them.

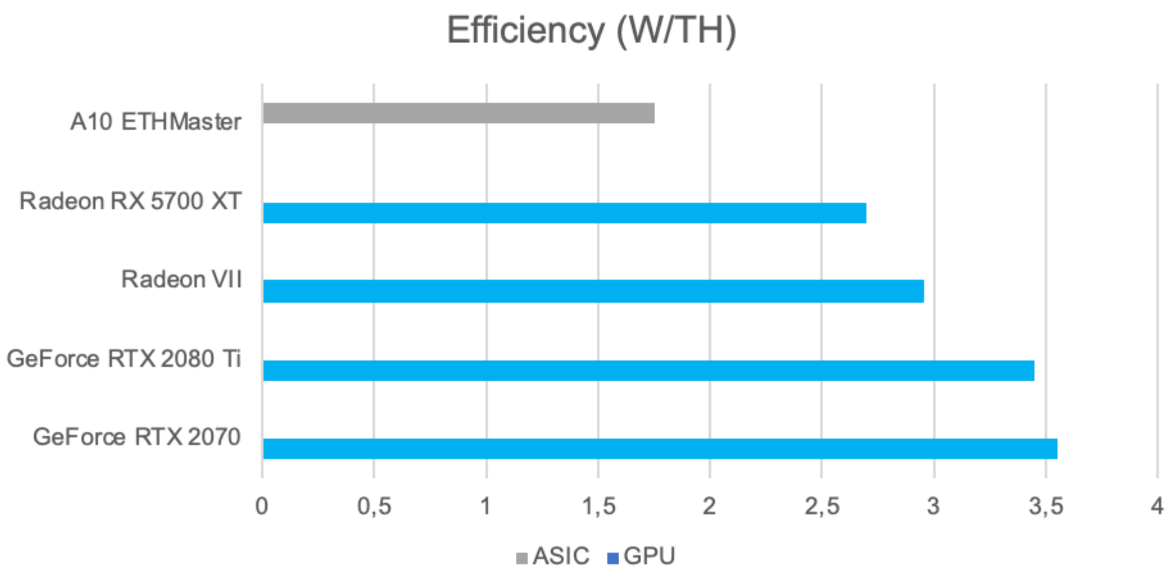


Figure 4. Efficiency: GPU vs. ASIC miners (Ethereum mining)

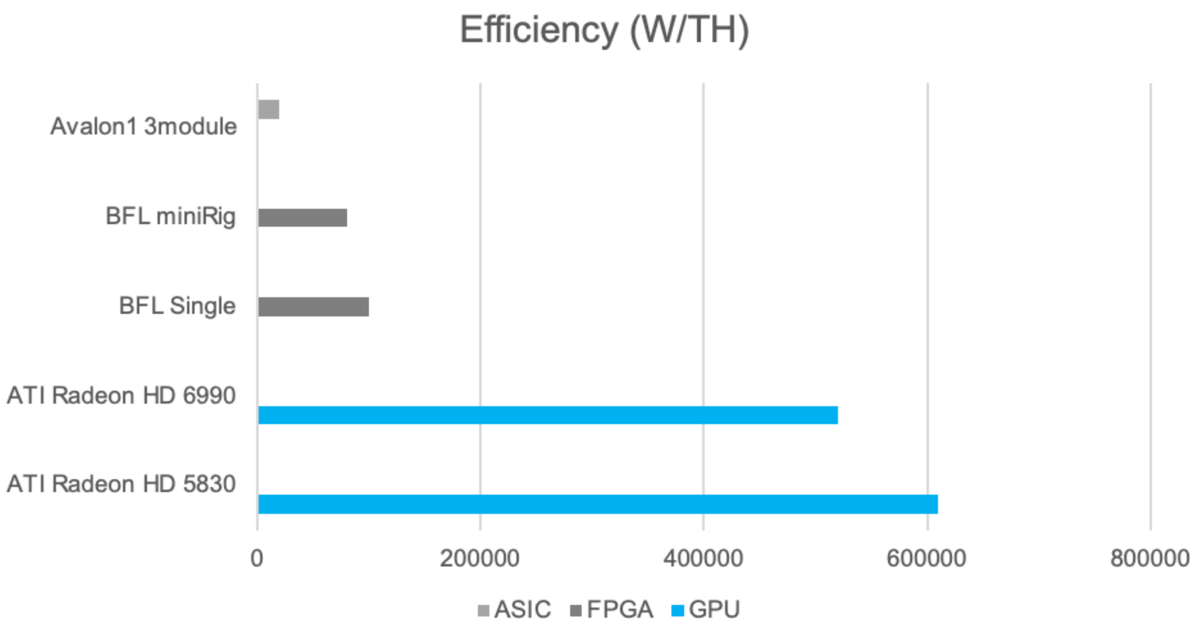


Figure 5. Efficiency: GPU and FPGA vs. ASIC miners (Bitcoin mining)

To analyse the energy consumption by the most popular mining infrastructure the manufacturers that are still in business and that have released machines since 2017 are shortlisted.

Manufacturer	Brand	Latest series
Bitmain	Antminer	S19
Bitfury	Bitfury	Tardis
Canaan	AvalonMiner	Series 12

It is important to analyse main characteristics of these machines.

Comparison of Recent Bitcoin ASIC Miner Machine Types

Machine	Hash rate (TH/s)	Power Consumption (Wh)	Power Efficiency (J/TH)
Antminer S19	95	3,250	34.5
Antminer T19	84	3,150	37.5
Antminer S19 Pro	110	3,250	29.5
Bitfury Tardis (Optimal CAPEX)	72	6,300	88
Bitfury Tardis Boost	100	6,300	63
AvalonMiner 1246	90	3,420	38
AvalonMiner 1166Pro	81	3,400	42
AvalonMiner 1146Pro	63	3,276	52
AvalonMiner 1166	68	3,196	47

Needless to underline **that mining hardware has evolved**, the above table depicts the improvement of both the hash rate and power efficiency, whereas the power consumption gradually decreases. The mining industry continues to evolve today, competition for bitcoin mining rewards will continue to spur technological evolution. As a result, mining machines will become more energy-efficient and less power-consuming.

In theory, having the main characteristics of the most popular and technical mining equipment it is possible to calculate the minimum level of energy consumption by the bitcoin network.

As mentioned above, Bitcoin difficulty rose as high as 155 million TeraHashes per second. The calculation of the minimum energy consumption level by a mining machine can be done by dividing 155 mln TH/s by each machine's hash rate. As shown in the table below 0.00458TWh is the minimum volume of consumed energy with the condition that all mining machines in the world are Antminer S19 Pro.

Of course, it is raw calculations as miners use different types of equipment and not all of those items consume the same amount of energy. However, this is an optimal representation of the minimum required level of energy to proceed bitcoins transactions.

Calculation of Energy Consumption

Machine	Items Needed to Mine BTC (based on difficulty), mln	Energy Consumption (TWh)
Antminer S19	1.631	0.0053
Antminer T19	1.845	0.0058
Antminer S19 Pro	1.409	0.00458
Bitfury Tardis (Optimal CAPEX)	2.152	0.0136
Bitfury Tardis Boost	1.55	0.00977
AvalonMiner 1246	1.722	0.0059
AvalonMiner 1166Pro	1.913	0.0065
AvalonMiner 1146Pro	2.460	0.008
AvalonMiner 1166	2.279	0.0072

To summarise the calculation of the minimum level of energy consumption, daily and yearly numbers should be considered. In the issue, lower bound consumption equals to 0.11 TWh per day or 40.12 TWh per year. In real-world terms the energy consumption of blockchains is difficult to make tangible. On the one hand, it should be noted that the same amount of electric energy is consumed by New Zealand every year. On the other hand, Bitcoin uses less than half the electricity as a banking system, and similarly pales in comparison to 241 Terawatts per hour consumed by the gold industry's mining operations.

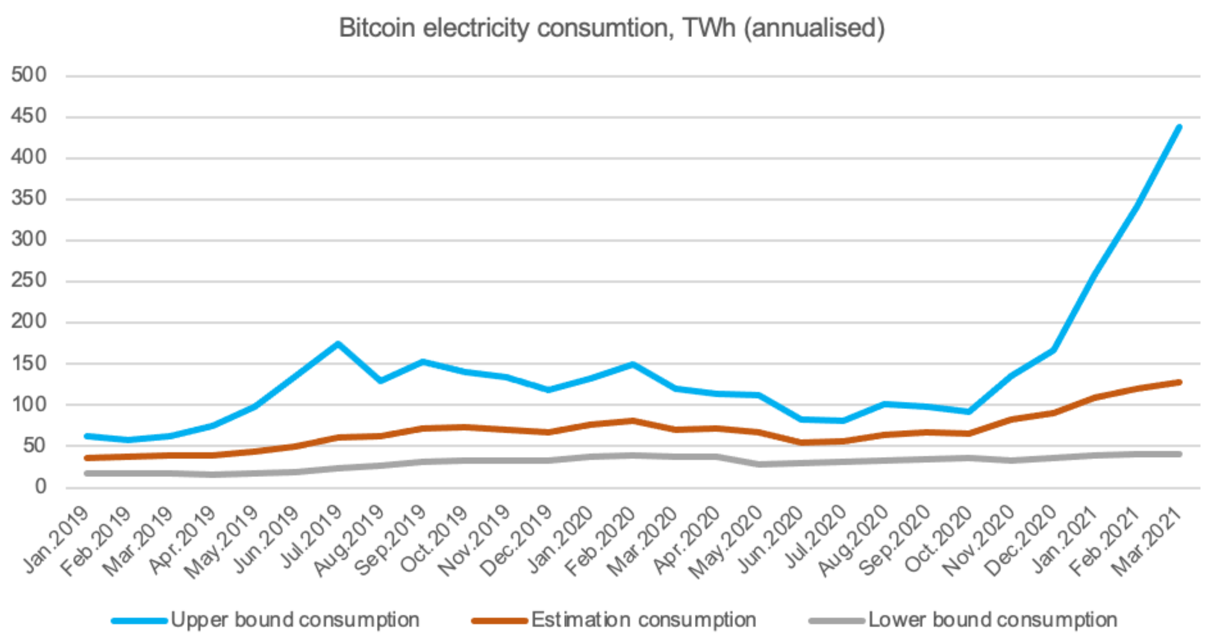


Figure 4: Bitcoin electricity consumption, TWh (annualised)

Based on [Cambridge University research](), the lower bound consumption is almost the same and equals to 40.46 TWh per year and the estimated consumption is 128 TWh. That exceeds the energy consumption level of such countries as Argentina, Norway, or the Netherlands.

As it was highlighted, based on the digiconomist analysis the carbon footprint of bitcoin energy consumption equals to 37.3 Mt CO_2 that is comparable to the carbon footprint of Trinidad and Tobago. As for Ethereum, carbon footprint is 12.35 Mt CO_2 that is the same as Panama emits.

Based on these analyses and data from IPO filings of hardware manufacturers and insights on mining facility operations and pool compositions, bitcoin mining is likely responsible for 10-20 Mt CO_2 per year, or 0.03-0.06% of global energy-related CO_2 emissions.

However, it should be mentioned that electricity generation in some bitcoin mining centres is dominated by renewables, including Iceland (100%), Quebec (99.8%), British Columbia (98.4%), Norway (98%), and Georgia (81%). Globally, CoinShares analysis estimates that the Bitcoin is powered by at least 74% renewable electricity as of June 2019.

Moreover, there are several strategies to achieve lower electricity costs and even levels of consumption:

1. Usage of renewable energy in general yields lower costs (as the electricity costs are lower), plus it is not harmful to the environment. The use of blockchain technology is growing at a rapid rate, leading to soaring energy consumption. Blockchain technology is secured and maintained by a vast network of miners to solve increasingly-complex computational problems. It's important that clean-energy technology is used to satisfy the rising blockchain ecosystem's usage needs. According to Bloomberg, the global power required to generate cryptocurrencies is equal to Argentina's entire electricity demand and serves as a growth engine for renewable energy producers from the United States to China.

2. Dynamic usage of data centres – as electricity cost varies during the day, it means to operate the data centre only when the electricity cost is lower, in that case, mining will yield more overall profit.

3. Usage of excess energy that cannot be stored – the cost goes to zero or in some cases the power manufacturers might even pay the data centre to use the extra energy as it must be used. Some countries have the problem of limiting the distribution of electricity from nuclear power plants. Consequently, the emergence of data centres in the area of nuclear power plants should solve the problem. Bitfury has entered a contract with the Ukrainian government to begin building data centres with this consideration of highest priority.

Section 4: Views from the Industry

INTERVIEW WITH WALTER KOK, CEO, ENERGY WEB

Walter Kok is CEO of the Energy Web Foundation. He brings nearly three decades of experience leading customer solutions and operational teams in complex, global organisational environments, including in the fields of fintech, telecommunications and information technology (IT). Prior to joining EWF originally as COO, Kok was COO of bank-wide operations at ING Bank, where he drove a series of transformation programmes and built a new type of operating model better equipped to deal with the challenges of regulatory requirements and technological disruption. In addition to ING, Kok's prior experience also includes senior board positions at Vodafone Global Enterprise, BT, NEC Corporation and several startups. He holds a Master's of Science in Digital Currency from the University of Nicosia and a Master of Science in computer systems networking and telecommunications from the Eindhoven University of Technology.

Question: What is Energy Web? What are you trying to achieve?

Energy Web is a global, mission-driven nonprofit accelerating the zero-carbon energy transition by harnessing the potential of public, open-source digital technology. Our technology stack includes both blockchain and other decentralised solutions as well as traditional, off-chain systems such as cloud-based IoT. The anchor of our tech stack is the Energy Web Chain, which launched in June 2019 as the world's first enterprise-grade blockchain tailored to the needs of the complex, highly regulated energy sector. In tandem, the Energy Web ecosystem has blossomed from an initial group of about ten affiliates when Energy Web was founded in 2017 to more than 100 companies globally today, comprising major energy companies, grid operators, renewable energy developers, automakers, and telcos. Together, we are building digital solutions that more fully tap into the value of zero-emissions distributed energy resources as a core component of the future energy system. Almost 50% of our members operate a validator node and actively contribute to operating our publicly accessible blockchain.

Question: There has been a lot of renewed debate so far this year about the high energy consumption of the Bitcoin blockchain. Also, there are voices debating about making blockchains "green". What is your personal take on this?

With the current conversation about blockchain energy consumption and making crypto green, we need to talk about two sides of a coin. On one hand, we have the issue of the energy efficiency and energy intensity of different blockchain networks. That's a demand-side topic. On the other hand, we have the related issue of powering blockchain operations with renewable energy. That's a supply-side topic.

With respect to the former issue—demand-side energy efficiency of blockchain networks—that highlights the important differences in various blockchains and how they achieve consensus. Bitcoin has of course made headlines for its energy-intensive Proof-of-Work approach to consensus. But many blockchains are migrating to energy-efficiency alternatives (such as Ethereum's move to Proof-of-Stake) or being built from scratch with energy efficiency baked into the platform (such as our Energy Web Chain, which uses Proof-of-Authority).

These energy-efficient alternatives are exciting, but let's also remember: debating whether Bitcoin might ever move to a PoW consensus alternative only focuses on half the equation: demand-side energy consumption. Regardless of any given blockchain's energy intensity and consumption, we still have the supply-side option: powering blockchains with 100% renewable energy. This is just as important, if not more so, and analogous to what we have seen happen in other industries.

For example, consider the built environment. Energy efficiency in buildings has been a hot topic for decades. Today, the two newer trends are a) electrifying remaining fossil-fueled energy demand (such as hot water and space heating) and b) sourcing that electricity demand from clean renewables. Crypto finds itself at a simple juncture: it is already electrified by virtue of being a digital currency. The energy efficiency of blockchain networks is under more scrutiny than ever before. Now the challenge before us is to ensure that the electricity powering blockchains is generated with renewables.

To be clear: the solution to making crypto green is *not* to mark individual tokens as green or not green. When you pay at the store with your Visa or Mastercard, there isn't 'green' credit and 'brown' credit. The underlying currency remains totally fungible. The same must remain true with cryptocurrencies like BTC and ETH. This is one of the primary benefits of crypto.

Question: You mentioned that Energy Web is building an enterprise-grade blockchain for the energy sector. How do you deal with energy efficiency and performance issues in such a highly demanding and highly complex sector?

The regulatory, market, and pure physical complexities of the world's power grids are some of the chief reasons why we launched the Energy Web Chain in the first place. From the outset, it was designed to be robust, fast, energy-efficient, and with low transaction costs.

Perhaps just as importantly, almost 50 companies and counting on four continents and 19 time zones host validator nodes that collectively maintain the network. Those companies go through a KYC vetting process, and the majority are grid operators and other legacy enterprises from the energy sector, including Eletrobras, Mercardos Eléctricos, Tenaska, and UTE in the Americas; Acciona, Elia Group, Engie, and Shell in Europe; and PTT Group, SB Energy, and SP Group in Asia.

Moreover, the Energy Web tech stack is not a blockchain-only solution. In addition to the foundational Energy Web Chain, we also leverage other decentralised digital technologies (such as for the utility services layer of our tech stack) as well as integrations with legacy IT systems (including SCADA and DERMs, in the case of grid operators).

But the far more important thing is not how the Energy Web tech stack works, but rather what it enables. A focus only on decarbonising crypto and blockchains misses the bigger picture: how this new generation of digital technology—including Energy Web's—can accelerate the global energy transition in a time of growing climate action urgency. That is the consistent theme behind all of Energy Web's work.

Question: You are leading Energy Web as the CEO. Which are in your opinion the most important challenges that your organisation will face in the future in its effort to scale up its solutions?

As we look ahead to the COP26 United Nations' climate change conference later this year in Glasgow, many are calling the 2020s the 'decisive decade' for global climate action. The energy transition needs to move a lot faster and achieve bigger emissions reductions sooner. Insofar as blockchain can help accelerate the energy transition, the biggest challenges we face are those that impede solutions from becoming adopted at scale fast.

In other words, the tech is already here. The Energy Web ecosystem alone has completed myriad successful pilots, proofs of concept, and early deployments with grid operators, energy companies, renewables developers, and electric vehicle stakeholders around the world.

For example, we've partnered on digital, blockchain-based renewable energy marketplaces in Asia with Minden in Japan, PTT Group in Thailand, SP Group in Singapore, and Foton in Turkey; in Europe with Engie in France and Accione and Iberdrola in Spain; and in the Americas with PJM in the United States, Mercados Eléctricos in El Salvador, and Eletrobras in Brazil. We can point to other examples for use cases such as virtual power plants, distributed energy resources providing grid flexibility, and digital 'passports' for lifecycle management of batteries. We know the technology performs. Now, how quickly can we scale adoption?

We see several key levers to make that happen, including: a) clearer regulations on crypto in general that are consistent across Europe and even better globally; b) standardisation around blockchain technologies in general (e.g., Energy Web is participating in standardisation bodies such as IEEE 2418.5 and EU-based initiatives, such as INATBA); and c) increasing utility comfort with digital tech overall, beyond blockchain specifically (e.g., utility investment in software 'infrastructure' has lagged investment in 'hard' poles-and-wires infrastructure. On this last point, we believe that a new era of decentralised service-level agreements (DSLAs) can help speed utility adoption of this new class of digital tech (i.e., blockchain).

For me, it is now down to a question of leadership. We need more executives and politicians to get out of their comfort zone and lead the way. I am in a fortunate position that a lot of our members are at the forefront of this transformation, but we need to go faster.

Question: Recently EW together with RMI and AIR launched the Climate Crypto Accord initiative. What is the vision of CCA? What are you trying to achieve?

The Crypto Climate Accord (CCA) is a private-sector-led initiative to decarbonise the crypto and blockchain industry. The fast-growing community of CCA Supporters now includes more than 45 companies spanning the crypto, finance, technology, NGO, and energy and climate sectors as a signal of support for developing solutions to decarbonise the crypto industry. More recently, we have also welcomed the first four Signatories, who make a public commitment to achieve net-zero emissions from electricity consumption associated with all of their respective crypto-related operations by 2030 and to report progress toward this net-zero emissions target using best industry practices.

Based on initial feedback from CCA Supporters, Energy Web has identified three activities that will underpin how Supporters make progress toward the CCA's objectives:

1. **Benchmarking & good industry practices:** Establish an enhanced baseline of the crypto industry's renewable energy use to bring greater clarity to this issue and define good industry practices based in alignment with renewable energy and carbon standards;
2. **Solution toolbox development:** Develop a toolbox of open-source solutions that help crypto holders directly decarbonise their crypto holdings and enable crypto networks to decarbonise from the bottom-up (more details here);
3. **Proof of progress:** Share measurable progress toward the CCA's objectives and highlight challenges where additional stakeholders are needed to lend support.

Our Supporters approve of the Accord's objectives and are involved with helping advise, develop, and scale solutions in support of the CCA. Becoming a CCA Supporter does not verify that a Supporter organisation has already decarbonised. The Crypto Climate Accord is also supported by the UNFCCC Climate Champions. Supporters are already developing solutions to convert the crypto industry's energy use into a new class of renewable energy buyers. For example, Energy Web will launch the first operational version of Energy Web Zero in Q1 2022 to provide crypto investors, holders, application developers, exchanges, and mining facilities a freely accessible and easy-to-use tool to buy verified renewables in an entirely digitised manner. In addition, bitcoin mining facility companies are beginning to explore the potential and needs for "green hash rate" software that can illustrate increasing renewable energy use by mining facilities.

Question: If you were asked to state your predictions for the future of scalability and performance of blockchain technology for the next 10 years, what would you say?

Blockchain technology is here to stay. There are many use cases being built now and already I can see the enormous potential for transforming the way people and businesses live and work around the world. I often compare where we are in the blockchain sector today with where we were with the Internet in 1995. The best is yet to come real impact on our day-to-day lives still has to be made.

Scalability is an important aspect of that. Not just from a technology perspective only but also from an ESG perspective. In my view, we will see many competing initiatives in the coming years around money and the different use cases there. Central Bank Digital Currencies, Bitcoin, Diem, other cryptocurrencies still to be developed. Decentralised Finance will be going through major scaling challenges too. I also expect the more common purpose chains (Ethereum, Polkadot, Cardano, and the likes) to tackle the challenges of how to scale in a more decentralised way, building the new internet.

When blockchains become a more integral part of the way we live our lives and do business we will automatically see the sector having to deal with existing laws and regulations. This can become a big issue when it comes to the speed of scaling this new infrastructure. Take a simple topic like the classification of the tokens. Is it a security, a utility, a payment token? These discussions take years and, in some countries, laws of 1931 are being applied to make an assessment. Clearly, our regulatory bodies also need to go back to the drawing table, understand the impact of this new technology and take a more pragmatic approach to how regulation will work in this new industry. From where I am sitting, I can see some countries really taking advantage by creating simple rules and a more agile approach to how the final regulations will be defined. I think this is very smart and will bring a lot of economic activity to these countries.

Energy Web has a unique position where we build an open-source, publicly accessible, digital infrastructure for the energy industry. To help decarbonise the electricity grid faster. We develop our stack with the sector, for the sector. I expect more of these sector-driven initiatives as it is really working very well. No vendor lock-in, an open environment for innovation and a public infrastructure that takes into account all relevant legislation like GDPR and others. The way we scale for our mission is by using our blockchain for what it does best: providing trust. All the services and common components that are relevant for the Energy Sector are built in the utility layer that is built on top of the trust layer. This allows us to scale, whilst honouring the principles of decentralised architectures and self-sovereign people and their energy assets.

We are ready for a future where hundreds of millions of energy devices with their own digital identity will form the new, customer centric electricity grid. Removing the need for carbon intensive electricity production. The sooner this becomes a reality, the better as far as I am concerned.

Section 5: Decarbonising Blockchains

INTRODUCTION

Cryptocurrencies like Bitcoin and Ether are becoming increasingly mainstream. And the primary technology underpinning the cryptocurrency industry—blockchain—is earning its place in dozens of industries, from healthcare to logistics to the energy sector.

Crypto demand is at an all-time high. Large enterprises are starting to accept cryptocurrencies as an alternative to conventional, fiat payment. Non-fungible tokens issued on top of blockchain platforms are supporting artisans in new and exciting ways. Meanwhile, major corporations and institutional investors have started adding cryptocurrencies to their balance sheets.

This surging demand for cryptocurrencies and the accelerating adoption of blockchain-based solutions have highlighted a critical issue: the technology's growing energy consumption and its impact on our climate.

The cryptocurrency industry is not alone in dealing with this dual energy-and-climate challenge. The technologies underpinning crypto are powered by electricity—just like other electricity-powered technologies such as cloud computing, data storage & processing, social networks, and artificial intelligence. Industries from across the global economy are beginning to decarbonise their operations in order to facilitate widespread, sustainable industry growth. That's why in April 2021 the Crypto Climate Accord (CCA) was born.

Inspired by the Paris Climate Agreement, the Accord is a private sector-led initiative for the entire crypto community focused on decarbonising the cryptocurrency industry in record time. Nonprofits Energy Web, the Alliance for Innovative Regulation, and RMI launched the CCA with more than 20 supporting organisations, including the UNFCCC Climate Champions, CoinShares, Consensys, Web 3 Foundation, Hut 8, Ripple, and the Global Blockchain Business Council.

There are three provisional objectives to be finalised in partnership with Accord supporters:

- Enable all of the world's blockchains to be powered by 100% renewables by the 2025 UNFCCC COP Conference;
- Develop an open-source accounting standard for measuring emissions from the cryptocurrency industry; and
- Achieve net-zero emissions for the entire crypto industry, including all business operations beyond blockchains and retroactive emissions, by 2040.

Activities under the Accord will be focused on quickly closing the gap between today's industry emissions and industry-wide decarbonisation for all blockchains, service providers, and other crypto industry activity, such as non-fungible tokens.

The Accord is organised around the following core principles:

- Build on existing forward progress: The electricity that powers our sector is decarbonising. Renewables have become cost-competitive in energy markets around the world. As a result, a growing share of the grid (and by extension our industry) is becoming cleaner;

- Mind the gap: recognise that significant work remains to be done. There is a substantial opportunity to close the gap between crypto emissions today and a net-zero emissions industry;
- Move quickly: Crypto's roots in open-source, agile, and technology innovation make crypto an ideal candidate to achieve something the world has yet to see: rapid industry-wide decarbonisation;
- Decentralised, open-source technology can accelerate progress: The same open-source, decentralised technology underpinning the global crypto industry — blockchain — can bring transformational levels of data transparency and trust to decarbonisation efforts;
- Voluntary, market-oriented, and value-added: Voluntary, private-sector led action on industry decarbonisation should be powered by a shared vision and market-driven solutions that accelerate market growth and create long-term value for everyone; and
- Community-driven: All crypto communities should work together, with urgency, to ensure crypto does not further exacerbate global warming but instead becomes a net positive contributor to the vital transition to a low carbon global economy. This process will be collaborative and based on shared interests and co-investment; no central body will dictate solutions.

HOW TO DECARBONISE BLOCKCHAINS

Blockchains are the single biggest source of energy consumption in the cryptocurrency industry. Yet given the decentralised nature of blockchains, how can they be decarbonised? Based on innovation already taking place today, we see two high-level paths to decarbonising them.

Supply side: leverage the innate transparency of blockchains to fully decarbonise from the bottom up.

The solution to making crypto green is not to mark individual tokens as green or not green. We want cryptocurrencies like BTC and ETH to remain 100% fungible. This is one of the primary benefits of crypto.

The real long-term solution is to ensure all blockchains are powered by 100% renewables. For some blockchains, the industry can achieve this by further investing in consensus mechanisms and solutions that are more energy-efficient (e.g., proof-of-stake). For other blockchains, the proof-of-work consensus is here to stay. In this space, the industry has an opportunity to leverage the transparency of blockchains themselves to measure just how much entire networks are powered by renewables.

Today, innovative companies are launching crypto mining sites in areas rich with renewables and in some cases using crypto mining to absorb renewable electricity that would otherwise be lost. To accelerate green mining further, we can use open-source technology to measure and report — on a completely anonymous basis — how much mining is green.

Strong precedent exists: renewable energy certification schemes are already active in markets across the globe that track renewable power generation. We can use a similar approach here to measure renewable power consumption tied to crypto mining activities.

This concept is almost identical to what technology giants Microsoft and Google are currently experimenting on with regards to data centres. Their intention is to prove that their data centres are being powered twenty-four hours a day, seven days a week by renewable energy. We can apply a similar technology approach to the crypto industry. If successful, crypto producers will be able to verifiably claim and prove their contribution to making an entire blockchain green—all while maintaining complete privacy for the businesses involved in crypto production

Under the Accord, we will support development of open-source software that crypto producers, together with grid operators and renewable energy companies, can install to prove the origin of the electricity they use to mine crypto. This software will in turn help miners build stronger relationships with local/regional/national policymakers and regulators since they can use the proof of their renewable energy procurement to show their support for decarbonisation efforts and eliminate concerns among policymakers and regulators about their energy use.

This technology—paired with governance structures that already exist in the renewable energy industry—can enable the entire industry to track and prove the green-ness of entire blockchains.

Demand side: enable crypto investors and users to decarbonise their crypto holdings from the top down.

Corporates around the world are already decarbonising their businesses using renewable electricity.

According to the RE 100 — a global initiative of nearly 300 large corporates committed to 100% renewable electricity — these companies are driving over 315 terawatt-hours of renewable electricity demand per year (for comparison, the BTC network uses ~120 terawatt hours / year according to the Cambridge Bitcoin electricity consumption index).

The same products used by these companies to decarbonise their businesses can be applied to the crypto industry. Corporates, institutional investors, and even retail cryptocurrency holders can choose to purchase renewable energy that is directly tied to their crypto.

Depending on the geography and crypto investor preferences (around price, impact, etc.), there are many renewable energy options to choose from. In the end, crypto investors receive energy attribute certificates reflecting the proof of their renewables' procurement from existing or not-yet-built renewable energy facilities, from local or highest-impact geographies (e.g., off-grid or conflict zone context), and bundled or unbundled with their electricity bills from their electric utility to name a few.

Here are two examples:

A major corporate or institutional crypto investor with strong sustainability commitments calculates the amount of non-renewable electricity attributable to their current cryptocurrency holdings. They then enter into a bilateral agreement with a renewable energy developer to purchase renewables over a multi-year period. The size of the project is directly correlated to the amount of non-renewable electricity used behind their crypto holdings.

A retail crypto investor purchasing crypto through an exchange chooses a "green crypto" option. This option charges a small percentage on top of the crypto transaction and places that value into an escrow account. This account is then used to purchase renewables from qualified renewable energy projects just like the corporate example above.

In both cases, open-source technologies can be used to link these transactions to specific renewable energy projects around the world in order to prove their impact on decarbonising crypto.

The Accord will be used as a coordinating framework to help crypto and renewable energy market participants deploy solutions like these,

THE PATH FORWARD

The Accord's collective ambition will create wins for both the planet and the global economy. Throughout the rest of 2021, Accord founders will:

- Engage a broad variety of crypto stakeholders to profile existing solutions for industry decarbonisation and identify areas for further innovation,
- Help crypto holders decarbonise existing crypto holdings via mature renewable energy products and services already in-use by other industries around the world,
- Bring verified renewables to crypto mining and production at a global scale,
- Report on the Accord's impact, and
- Host the inaugural Crypto Climate Accord Congress.

Section 6: Policy Recommendations

This section proposes a set of policy recommendations based on the topics addressed in this thematic report.

RECOMMENDATIONS

- **Energy efficiency**
  At the EU level, the European Blockchain Services Infrastructure needs to consider the energy consumption (and efficiency) of blockchain when deciding on the underlying technology for developing the necessary digital infrastructure. At a Member State level, national blockchain-based deployments should also be transparent on their energy consumption. As also discussed in Section 1 of this report, blockchain solutions based on the Proof-of-Work consensus mechanisms should be avoided due to their significantly higher energy consumption compared to other consensus protocols, such as the Proof-of-Stake or Proof-of-Authority for example. Also, considering publicly accessible blockchain solutions using a limited number of validator nodes (e.g., public consortium-based blockchains based on Proof-of-Authority) can also be a way of providing the necessary trust and performance while preserving energy efficiency.
- **Scalability and performance**
  The topic of energy efficiency of blockchain-based solutions should also be considered under the light of scalability and performance on the underlying blockchain technologies. It is quite common that energy consumption increases exponentially when applications move from the proof-of-concept phase into production. Therefore, it is recommended that energy efficiency-related issues need always to be treated along with the scalability and performance requirements of the blockchain-based solution under evaluation. As presented in Section 1 of this report and further analysed in Section 3, scalability and performance are closely related to the type of the underlying consensus mechanism in use. To this extent and in order to meet the necessary performance needed by specific applications, one may consider using a limited number of validators following publicly accessible Proof-of-Authority blockchain solutions.
- **Use of renewable energy**
  Since energy consumption is an intrinsic aspect of applications based on blockchain technology, it is important to make sure that renewable energy is used to the maximum possible extent to cover the demand for energy. In the EU, the Guarantees of Origin (GOs) serve as the Energy Attribute Certificates. However, GOs reflect average consumption and production over longer time periods, in practice a year. Therefore, they do not take into account when the production and consumption take place, thus they consider the total in the time period, not the consumption or production patterns within it. To implement a more efficient mechanism for the use of renewable energy for blockchain operations, a 24/7 hourly matching of consumption and production of renewables schemes need to be in place. This means that we would be in the position to know if the consumption matches renewable production every day, every hour. Several initiatives are currently trying to compensate for the energy consumption of the Proof-of-Work blockchains, and especially those related to Bitcoin, that require the purchase of Energy Attribute Certificates from the miners according to their energy consumption. Such an initiative called Crypto Climate Accord is presented and discussed in Section 5 of this report.
- **Certification**
  Certification of equipment used as infrastructure for the deployment of public-sector blockchain solutions at a European and Member State level should be in place. These certifications may take the form of an “Energy Performance Certification” similar to the ones already applied in Europe and are related to building, equipment, or infrastructure. This process should be based on the benchmarking of the equipment used in mining facilities as analysed and presented in Section 3 of this report.

- **Energy efficiency evaluation criteria**
  It is recommended that specific evaluation criteria related to the performance and energy efficiency of blockchain-based solutions for the public sector need to be specified at European and Member State level. These criteria could also be used to evaluate the performance in terms of energy consumption not only of existing solutions but also can become part of the evaluation process of public tenders at a European or Member State level that are requesting blockchain-based solutions as part of the technical specification of the tender. This way, a common and standardised European framework for assessing the energy consumption of public sector blockchain-based solutions can be developed. This process is also closely related to the certification process of the equipment used in mining facilities as discussed in Section 3 of this report.
- **Blockchain energy consumption index**
  To assess the energy consumption of blockchain-based solutions in an independent and unbiased manner, a blockchain energy consumption index should be developed and agreed upon between the Member States. The blockchain energy consumption index should leverage the available information on the energy balance for each Member State to also provide insights on the type of energy that is used to power the blockchain solutions at a European and Member State level. Moreover, the blockchain energy consumption index should also try to model the energy consumption of other blockchains apart from Bitcoin.
- **Guidance and knowledge sharing**
  Create programmes for knowledge-sharing and dissemination of pilot results and best practices on blockchain deployments between the Member States. Moreover, guidance should also be provided along with guidelines and recommendations to foster and promote the knowledge around the topic of the energy efficiency of blockchain technology.

Finally, it should be mentioned that in China, the State Council's Financial Stability and Development Committee stated in May 2021 that it will ban Bitcoin mining and trading activities as part of efforts to fend off financial risks [33]. Moreover, a crackdown on cryptocurrency "mining" has extended to the southwest province of Sichuan, where authorities ordered cryptocurrency mining projects closed in the major mining centre [34]. This development’s importance, if this development is justified, forms the fact that China accounts for more than half of global Bitcoin production.

In this context, the Sichuan Provincial Development and Reform Commission, and the Sichuan Energy Bureau issued a joint notice in June 2021, demanding the closure of 26 suspected cryptocurrency mining projects within a couple of days. It should also be mentioned that Sichuan is China's second-biggest Bitcoin mining province, favored by the fact that several miners move their rigs in Sichuan to benefit from the rich hydropower resources of the province during the summer period. According to this notice, state-owned electricity suppliers have been ordered to conduct inspections to their customers and to immediately terminate the supply of electricity to crypto mining facilities. This is mainly driven from the fact that apart from Sichuan, in other popular mining regions, such as Inner Mongolia, the crypto mining industry heavily uses electricity produced by means of highly polluting sources, such as coal [34].

Similar to the province of Sichuan, other Chinese mining hubs mainly located in Inner Mongolia, Xinjiang, Yunnan and Sichuan, have unveiled detailed measures to root out the crypto mining industry [34].

Chinese authorities state that cryptocurrencies disrupt economic order and facilitate illegal asset transfers and money laundering [33], [34], [35].

REFERENCE LIST

1. Blandin, A. et al., 2020. 3rd Global Cryptoasset Benchmarking Study - CCAF publication. *Cambridge Centre for Alternative Finance, Cambridge University, Judge Business School*. Available at: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/3rd-global-cryptoasset-benchmarking-study/ [Accessed March 13, 2021].
2. CCAF, 2019. CBECI. *Cambridge Bitcoin Electricity Consumption Index (CBECI)*. Available at: https://cbeci.org/faq/ [Accessed March 13, 2021].
3. de Fries, A., Digiconomist, Bitcoin Energy Consumption Index. *Digiconomist*. Available at: https://digiconomist.net/bitcoin-energy-consumption [Accessed March 13, 2021].
4. Peyravi, R. & Girard, G., 2021. CCAF.
5. Dek, A., 2021. CCAF.
6. de Fries, A., Ethereum Energy Consumption Index (beta). *Digiconomist*. Available at: https://digiconomist.net/ethereum-energy-consumption [Accessed March 11, 2021].
7. Helmy, K. & Coinmetrics, 2020. Issue 51 - The Half-Time Show: The State of Bitcoin Network Security After the Halving. *Coin Metrics' State of the Network*. Available at: https://coinmetrics.substack.com/p/coin-metrics-state-of-the-network-fcf [Accessed March 10, 2021].
8. Aublin, P.-L., Mokhtar, S.B., Quéma, V., 2013. RBFT: Redundant Byzantine Fault Tolerance, in: 2013 IEEE 33rd International Conference on Distributed Computing Systems. Presented at the 2013 IEEE 33rd International Conference on Distributed Computing Systems, pp. 297–306. https://doi.org/10.1109/ICDCS.2013.53
9. Beekhuizen, C., 2021. A country's worth of power, no more! [WWW Document]. URL https://blog.ethereum.org/2021/05/18/country-power-no-more/ (accessed 8.11.21).
10. Buterin, V., 2014. A NEXT GENERATION SMART CONTRACT & DECENTRALISED APPLICATION PLATFORM 36.
11. Butijn, B.-J., Tamburri, D.A., Heuvel, W.-J. van den, 2020. Blockchains: A Systematic Multivocal Literature Review. ACM Comput. Surv. 53, 1–37. https://doi.org/10.1145/3369052
12. Canetti, R., Garay, J.A. (Eds.), 2013. Advances in Cryptology – CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II, Lecture Notes in Computer Science. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40084-1
13. Castro, M., Liskov, B., 1999. Practical Byzantine Fault Tolerance 14.
14. David, B., Gaži, P., Kiayias, A., Russell, A., 2018. Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain, in: Nielsen, J.B., Rijmen, V. (Eds.), Advances in Cryptology – EUROCRYPT 2018, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 66–98. https://doi.org/10.1007/978-3-319-78375-8_3
15. De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., Sassone, V., 2017. PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain 11.
16. de Vries, A., 2018. Bitcoin's Growing Energy Problem. Joule 2, 801–805. https://doi.org/10.1016/j.joule.2018.04.016
17. European Commission, 2021. Commission proposes a trusted and secure Digital Identity [WWW Document]. European Commission - European Commission. URL https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663 (accessed 8.10.21).
18. Gallersdörfer, U., Klaaßen, L., Stoll, C., 2020. Energy Consumption of Cryptocurrencies Beyond Bitcoin. Joule 4, 1843–1846. https://doi.org/10.1016/j.joule.2020.07.013
19. Gilad, Y., Hemo, R., Micali, S., Vlachos, G., Zeldovich, N., 2017. Algorand: Scaling Byzantine Agreements for Cryptocurrencies, in: Proceedings of the 26th Symposium on Operating Systems Principles. Presented

at the SOSP '17: ACM SIGOPS 26th Symposium on Operating Systems Principles, ACM, Shanghai China, pp. 51–68. https://doi.org/10.1145/3132747.3132757

20. Krause, M.J., Tolaymat, T., 2018. Quantification of energy and carbon costs for mining cryptocurrencies. Nat Sustain 1, 711–718. https://doi.org/10.1038/s41893-018-0152-7
21. Lei, N., Masanet, E., Koomey, J., 2021. Best practices for analysing the direct energy use of blockchain technology systems: Review and policy recommendations. Energy Policy 156, 112422. https://doi.org/10.1016/j.enpol.2021.112422
22. Mora, C., Rollins, R.L., Taladay, K., Kantar, M.B., Chock, M.K., Shimada, M., Franklin, E.C., 2018. Bitcoin emissions alone could push global warming above 2°C. Nature Clim Change 8, 931–933. https://doi.org/10.1038/s41558-018-0321-8
23. Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system.
24. Ongaro, D., Ousterhout, J., 2014. In Search of an Understandable Consensus Algorithm 16.
25. Paypal, 2020. Global Impact Report. Highlights 52.
26. Poon, J., Dryja, T., 2016. The Bitcoin Lightning Network: 59.
27. Roşu, I., Saleh, F., 2021. Evolution of Shares in a Proof-of-Stake Cryptocurrency. Management Science 67, 661–672. https://doi.org/10.1287/mnsc.2020.3791
28. Saltini, R., Hyland-Wood, D., 2019. IBFT 2.0: A Safe and Live Variation of the IBFT Blockchain Consensus Protocol for Eventually Synchronous Networks. arXiv:1909.10194 [cs].
29. Sedlmeir, J., Buhl, H.U., Fridgen, G., Keller, R., 2020a. The Energy Consumption of Blockchain Technology: Beyond Myth. Bus Inf Syst Eng 62, 599–608. https://doi.org/10.1007/s12599-020-00656-x
30. Sedlmeir, J., Buhl, H.U., Fridgen, G., Keller, R., 2020b. Ein Blick auf aktuelle Entwicklungen bei Blockchains und deren Auswirkungen auf den Energieverbrauch. Informatik Spektrum 43, 391–404. https://doi.org/10.1007/s00287-020-01321-z
31. Visa, 2019. Corporate Responsibility & Sustainability Report 52.
32. Vranken, H., 2017. Sustainability of bitcoin and blockchains. Current Opinion in Environmental Sustainability 28, 1–9. https://doi.org/10.1016/j.cosust.2017.04.011
33. "China vows to crack down on bitcoin mining, trading activities", Reuters, May 2021, https://www.reuters.com/technology/china-says-it-will-crack-down-bitcoin-mining-trading-activities-2021-05-21/
34. "China's cryptocurrency-mining crackdown spreads to Sichuan", Reuters, June 2021, https://www.reuters.com/technology/chinas-cryptocurrency-mining-crackdown-spreads-sichuan-2021-06-19/
35. "China's ban forces some bitcoin miners to flee overseas, others sell out", Reuters, June 2021, https://www.reuters.com/technology/chinas-ban-forces-some-bitcoin-miners-flee-overseas-others-sell-out-2021-06-25/

Annex

COMPARISON OF CONSENSUS PROTOCOLS

Firstly, we have to dive into what Consensus means and what algorithms mean, how a combination of them is bringing Consensus Protocols based on an automated process for a multiparty scenario, not only involvement rather than consequences in effect of a fact with responsibilities behind. A **distributed consensus** mechanism starts with no leader and it establishes **trust between the stakeholders** which includes the exchange of proofs and values.

Consensus Protocols can be divided into **two major families**, and a comparison could be understandable from the problems they afront and solve in a different manner.

- Those existing **before Bitcoin**, Byzantine based consensus;
- Those that only exist **after Bitcoin**, family of Nakamoto consensus;

Byzantine general´s problem, addressed in 1982 by Leslie Lamport, Robert Shostak and Marshall Pease:

“Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach an agreement. It is shown that using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so, a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors”.

This family is called Byzantine fault-tolerant protocols whereby there are algorithms that are robust enough for random types of failures in a distributed manner with which a Byzantine Agreement protocol is commonly adopted. There are two basic consensuses in a different way, those based on a **lottery** and those based on **election**.

In 1985, Michael Fisher, Nancy Lynch and Michael Patterson “Impossibility of Distributed Consensus with One Faulty Process” and their job is called FLM impossibility whereby demonstrated that every protocol has the possibility of non-termination, “even with only one faulty process” where asynchronous systems are needed and some of them are unreliable, in contrast with synchronous cases where Byzantine general´s problem is solved efficiently. These aspects essentially raised the Consistency, Availability, Partition tolerance theorem approach where properties are Consistency, Availability, and tolerance to Partitioning. Although in 2002 Seth Gilibert and Nancy Lynch demonstrated that **Coherence** can be relaxed in a partially synchronous distributed network to secure Availability and Partitioning.

The famous FLP impossibility problem is essential for Richard Guerraoui, Matej Pavlovic and Drago-Adrian Seredinschi in their work, with which they present the problem based on the state machine replication and consensus whereby the adversary can control various parts of the system with two assumptions: behaviour (how much control the adversary has over the nodes´ behaviour) and Synchrony (how much control has over the message transmission delays and delivery guarantees of the network) which conclude into a question *“What is necessary to compromise the liveness and/or safety of a blockchain protocol?”* and consume their questions with **A-indulgent** protocols (maintaining safety while minimal restrictions on the adversary in synchrony) or **B-indulgent** protocols (which are indulgent towards malicious nodes although require additional synchrony to remain safe).

Both families differ in a critical aspect, nodes in PBFT choose leaders and commit on values after consulting with a majority of the system and Nodes in Bitcoin commit on a value after some time passed and accumulate the value confirmations where relies on timing assumptions. Although raised three elemental properties which are validity, agreement and termination.

There is a very interesting survey by IEEE on Consensus Mechanism and Mining Strategy Management in Blockchain Networks distinguishes three properties of Nakamoto Protocols in comparison with the Byzantine agreement: common-prefix property, Chain-quality property and Chain-growth property within a context of primitive PoW scheme whereby its correspondences as agreement, validity and liveness in the context of Byzantine Agreements allow reaching a wide variety of PoW Schemes for Permissionless Blockchains. https://arxiv.org/pdf/1805.02707.pdf (TABLE III).

The properties of the consensus protocol allow to evaluate the node´s behaviour in particular the validator nodes with which Integrity, authentication, termination, and independence are the main criteria aborded by the Study Report by ISO TC 307 on regards to Security Evaluation of Consensus Models; however, it is extremely interesting mixed properties and hybrid consensus protocols based on incentive capabilities, not only economic incentives.

At the deliverables of ITU-T FG DLT in 2019, the Technical Report D.5.1. Outlook on DLT presented another Comparative table, TABLE 4 which compares based on properties as safety and performance.

Table III
COMPARISON OF DIFFERENT POX SCHEMES FOR PERMISSIONLESS BLOCKCHAINS

Puzzle Name	Origin of Hardness (One-way Function)	Designing Goal	Implementation Description	ZKP Properties	Simulation of Random Function	Features of Puzzle Design	Network Realization
Primitive proof of work [23], [86]	Partial preimage search via exhaustive queries to the random oracle	Sybil-proof	Repeated queries to cryptographic hash function	Yes	Yes	Single challenge	Bitcoin [1], Litecoin [92]
Proof of exercise [105]	Matrix product	Computation delegation	Probabilistic verification	N/A	No	Single challenge	N/A
Useful proof of work [84]	K-orthogonal vector, 3SUM, all-pairs shortest path, etc.	Computation delegation	Non-interactiveness via Fiat-Shamir transformation	Yes	Yes	Single challenge with sequential hash queries	N/A
Resource-efficient mining [100]	N/A	Computation delegation	Guaranteed by TEE	Yes	Yes	Trusted random oracle implemented by dedicated hardware	N/A
Proof of retrievability [110]	Merkle proofs of file fragments in the Merkle tree	Distributed storage	Non-interactiveness via Fiat-Shamir transformation and random Merkle proofs	Yes	Conditional	Two-stage challenge	Permacoin [109], KopperCoin [70]
Proof of space -time [36]	The repeated proof of retrievability over time	Decentralized storage market	Repeated PoR	Yes	Conditional	Two-stage challenge and repeated PoR over time	Filecoin [36]
Equihash [81]	The generalized birthday problem	ASIC resistance	Time-space complexity trade-off in proof generation [81]	Yes	Yes	Memory-hard	ZCash [44]
Ethash [114]	Random path searching a random DAG	ASIC resistance	Repeated queries to cryptographic hash function	Yes	Yes	Sequential, memory-hard puzzle	Ethereum [35]
Nnonoutsourceable scratch-off puzzle [82]	Generalization of proof of retrievability	Centralization resistance	Random Merkle proof	Yes	Yes	Two-stage challenge	N/A
Proof of space [116]	Merkle proofs of a vertex subset in a random DAG	Energy efficiency	Random Merkle proof	Yes	Yes	Two-stage challenge and measurement of proof quality	SpaceMint [116]
Proof of human work [102]	Radom CAPTCHA puzzle requiring human effort	Useful work and energy efficiency	CAPTCHA and PoW	Yes	Yes	Human in the loop	N/A

Figure 1: Comparison of Different PoX Schemes for Permissionless blockchains by Wang et al.

Figure 2: Comparative analysis of consensus schemes

Table 4: Comparative analysis of consensus schemes

	Systems	Committee Formation (Resources)	Strong Consistency	Single Committee				Multiple Committee			Safety			Performance			
				Committee Configuration	Inter-Committee Consensus			Intra-committee Configuration	Intra committee Consensus								
					Incentives (Join,Par-ticipate)	Leader	Msg.		Mediated	Incentives	Transaction Censorship Res.	DoS Res.	Adversary Model	Throughput	Scalable	Latency	Exp. Setup
Hybrid	ByzCoin [b-Kogias]	PoW	√	Rolling (singl)	√ ×	Internal	O(n)	/	/	/	√	part	33%	1000 tx/s1	×	10–20s 1	Real
	Solidus [b-Abraham]	PoW	√	Rolling (singl)	√ √	External	O(n2)	/	/	/	×	part	33%	/	/	/	/
	Algorand [b-Gilad]	Lottery	√	Full swap	××	Internal	O(n2)	/	/	/	×	√	33%	90 tx/h 2	×	40s 2	Real
	Hyperledger [b-Vukolic-b]	Permissioned	√	Static	/	Flexible	Flexible	/	/	/	√	√	33%	110k tx/s 3	×	<1s 3	Real
	Tencent TrustSQL	Permissioned	√	Static	/	/	/	/	/	/	√	√	50%	50k+tx/s 12	×	20ms 12	Real
	RSCoin [b-Danezis]	Permissioned	√	Static	/	Internal	O(n)	×	Client	×	√	√	33%	2k tx/s 4	√	<1s 4	Real
	Elastico [b-Luu]	PoW	√	Full swap	√ ×	Internal	O(n2)	Dynamic (Random)	!	!	×	√	33%	16 blocks/110s 5	√	110s/ 16 blocks	Real
	Omniledger [b-Kogias-b]	PoW/PoX	√	Rolling (subset)	√ ×	Internal	O(n)	Dynamic (Random)	Client	×	√	√	33%	≈10k tx/s 6	√	≈1s 6	Real
	Chainspace [b-Bassam]	Flexible	√	Flexible	××	Internal	O(n2)	×	×	×	√	part	33%	350 tx/s 7	√	<1s 7	Real
Proof-of-X	Ouroboros [b-Kiayias]	Lottery	×	Full swap	√ √	Internal	O(nc)	/	/	/	×	√	50%	257.6 tx/s 9	×	20s	Simulation
	Praos [b-David]	Stake	×	Rolling (subset)	√ √	Internal	O(1)	/	/	/	×	part	50%	/	/	/	/
	Snow-white [b-Daian]	Stake	×	Full swap	√ √	Internal	O(1)	/	/	/	×	√	50%	100-150 tx/s 9	√	?	Simulation
	PermaCoin [b-Miller]	PoW/PoR11	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	50%	/	×	/	/
	SpaceMint [b-Hønsi]	PoS	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	50%	?	×	600s	Simulation
	Intel PoET [b-Intel]	TH12	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	TH12	1000 tx/s 10	√	/	Real
	REM [b-Zhang]	TH12	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	TH12	!	√	/	Real
Proof-of-work	Bitcoin [b-Nakamoto]	PoW	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	50%	7 tx/s	×	600s	Real
	Bitcoin-NG [b-Eyal]	PoW	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	part	50%	7 tx/s	×	<1s	Simulation
	GHOST [b-Sompolinsky-b]	PoW	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	50%	/	×	/	/
	DECOR+HOP [b-Lerner]	PoW	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	50%	30 tx/s 8	×	60s	Simulation
	Tencent TrustSQL	PoW	√	Rolling (singl)	× √	Flexible	O(1)	/	/	/	√	√	50%	50k+ tx/s 12	×	50ms	Real
	Spectre [b-Sompolinsky-a]	PoW	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	50%	/	×	/	/

1 144 nodes/committee.
2 50k nodes/committee.
3 4 nodes/committee (corresponding to BFTSmart [b-Kim]) corresponding to HyperLedger v0.6, new consensus scheme [b-Thakkar] is used after v0.6.
4 3 nodes/committee. 10 committees.
5 100 nodes/committee. 16 committees.
6 72 nodes/committee (12.5% adversary). 25 committees.
7 4 nodes/committee. 15 committees.
8 1 minute average interval; 1 block = 1 MB.
9 40 nodes.

Every consensus protocol can offer a different property or a set of properties to the network. There are examples like Bitcoin where mining is required to add a block in the chain, while other examples are not relying on mining and implement a minting system to add a block in the chain based on transactions. The latter examples contemplate numerous cases that apply an election or voting mechanism. The following figure briefly includes these examples.

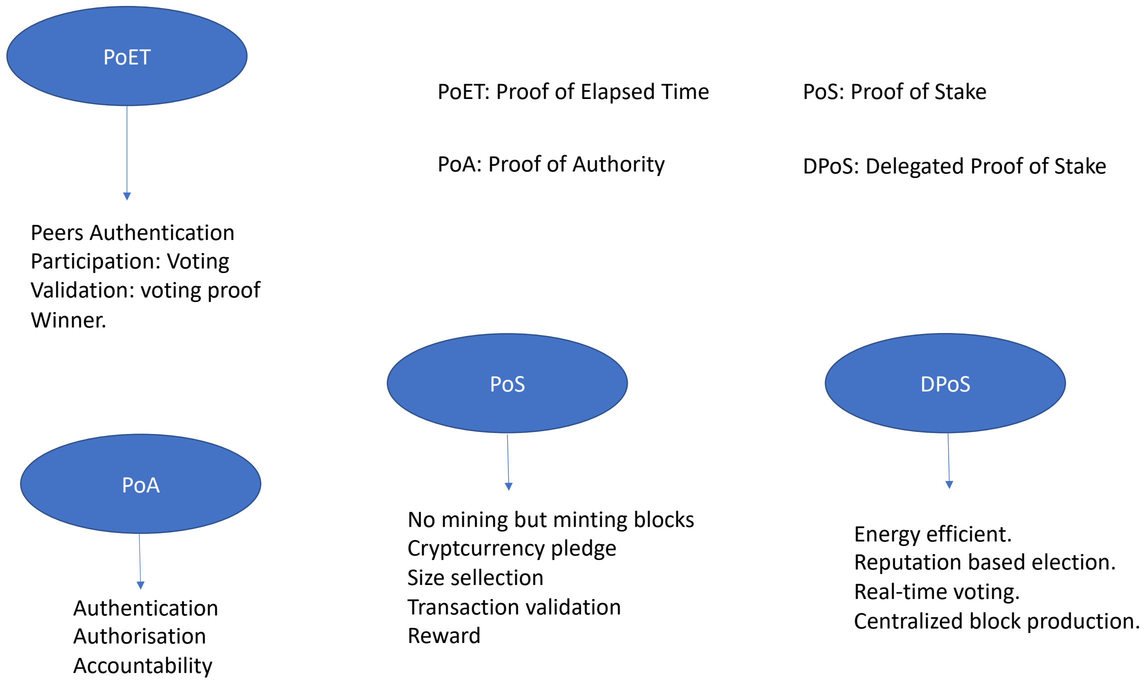


Figure 3: Summarisation of consensus algorithms and properties