Review Article

Evaluation of Green Alternatives for Blockchain Proof-of-Work (PoW) Approach

Mahdi H. Miraz[1,2,3], Peter S. Excell[2] and Khan Sobayel[4,*]

[1]Xiamen University Malaysia, Malaysia
m.miraz@ieee.org
[2]Wrexham Glyndŵr University, U.K.
p.excell@glyndwr.ac.uk
[3]The Chinese University of Hong Kong, Hong Kong SAR
[4]The National University of Malaysia, Malaysia
sobayel@ukm.edu.my
*Correspondence: sobayel@ukm.edu.my

Received: 20th August 2021; Accepted: 25th September 2021; Published: 1st October 2021

Abstract: Following the footprints of Bitcoins, many other cryptocurrencies were developed mostly adopting the same or similar Proof-of-Work (PoW) approach. Since completing the PoW puzzle requires extremely high computing power, consuming a vast amount of electricity, PoW has been strongly criticised for its antithetic stand against the notion of green computing. Use of application-specific hardware, particularly application-specific integrated circuits (ASICs) has further fuelled the debate, as these devices are of no use once they become "legacy" and hence obsolete to compete in the mining race, thus contributing to electronics waste. Therefore, this paper surveys the currently available alternative approaches to PoW and evaluates their applicability - especially their appropriateness in terms of greenness.

Keywords: *Application-specific integrated circuit (ASIC); Blockchain; Blockchain mining; Carbon footprint; Green computing; Greenhouse gas emission (GHGE); Information and communication technology (ICT); Proof-of-Stake (PoS); Proof-of-Work (PoW)*

1. Introduction

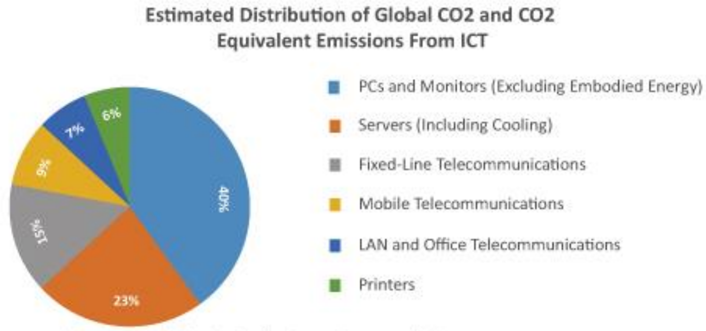
Our personal, professional and societal life is now greatly enriched by the usage of Information and Communication Technology (ICT). Despite many benefits that ICT has been bringing to enhance and improve people's lives, there are also many negative factors. One of the major downsides is the carbon footprint produced by the ICT sector, mainly due to exponentially increasing consumption of energy at different stages of the life-cycle. According to the U.S. Environmental Protection Agency, production of electricity and the transportation sector contributed approximately 28% each to the total greenhouse gas emissions in 2016, while industry, residential & commercial and agricultural sectors contributed 22%, 11% and 9% respectively [1]. Superficially, it appears that ICT is not listed amongst the major contributors. However, if we consider the demand of energy needed for manufacturing and then powering the ICT devices, combined with their ubiquity in modern society, it is apparent that the ICT sector plays an important role in most of the categories mentioned above.

According to Pickavet *et al.* [2] the total global energy consumption of computers, networking equipment, data centres and other ICT devices (excluding smart devices) is projected to reach 14% by the year 2020. However, this does not consider the manufacturing contributions. In addition, the shorter life-

Mahdi H. Miraz, Peter S. Excell and Khan Sobayel, "Evaluation of Green Alternatives for Blockchain Proof-of-Work (PoW) Approach", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 54-59, Vol. 5, No. 4, 1st October 2021, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2021.04.005, Available: http://aetic.theiaer.org/archive/v5/v5n4/p5.html.

span of ICT devices, compared to other technologies, is another factor to consider. Another study, focusing on the contributions of smartphones, by Belkhir and Elmeligi [3] projects that by 2020, the carbon footprint solely produced by smartphones is highly likely to outstrip the distinct contributions of PCs, laptops and other display devices.

In 2015 Chinnadurai [4] reported that the ICT sector contributed approximately 2% of the overall carbon footprint. As a part of the whole, 2% may seem negligible, however, 2% here is equivalent to 0.86 billion tons, and this is forecasted to rise to 4% by 2020. A further break-down of this 2% contribution is demonstrated in fig. 1:



Note: Analysis does not include radio-broadcasting equipment or television.

Figure 1. Estimated Distribution of Global CO2 and Other Equivalent Emissions from ICT Sector [4]

These studies, however, did not significantly focus on the contribution by emerging crypto-currency mining trends which has become a major ICT-related environmental concern. Meeting the energy demand for cryptocurrency mining is significantly contributing towards fossil fuel consumption. The generation of energy, predominantly by fossil-fuel plants, to make and operate all the ICT devices on the market today is a significant contributing cause towards excess greenhouse gas emission (GHGE), through the creation of carbon dioxide (CO2).

By introducing the concept of Green Computing, this paper briefly explains how Proof-of-Work (PoW) operates, as used in blockchain ecosystems of cryptocurrencies such as Bitcoin, and then evaluates the greenness of the alternative approaches.

2. The Notion of Green Computing

In its simplest form, green computing mainly means the use of computing resources in an eco-friendly and environmentally responsible manner. The broader concepts also include the study and practice of many other aspects relevant to environmentally sustainable computing or IT, such as designing, engineering, manufacturing, disposing and using of computing resources in ways that help to reduce their overall impact on the environment. The terms green IT, green ICT, ICT sustainability are also used interchangeably.

Similar to any other green campaign, the aims of green computing remain the same, such as minimising energy consumption by optimising power efficiency over the products' lifecycle, reduction of use of hazardous materials in manufacturing, biodegradability and recyclability of the factory waste as well as the non-functioning or legacy products, such products ranging from small chips to devices used in large-scale data centres.

In fact, the notion of green computing was officially introduced by the U.S. Environmental Protection Agency as far back as 1992, by launching of Energy Star [5] - a government-backed voluntary labelling programme which was conceived for the purpose of promoting and recognising energy efficiency in electronic and electrical devices, including computing resources ranging from home appliances to industrial equipment. This was achieved by providing the buyers with unbiased credible information to help facilitate the making of well-informed purchase decisions. Another similar programme, known as "TCO Certified" was launched by the Swedish organization TCO Development, concurrent to Energy Star, by introducing the energy-saving "sleep mode" for computer displays. Although initially the programme was focused on promoting "low magnetic and electrical emissions from CRT-based computer displays" [6], it later expanded the scope by inclusion of other relevant criteria such as ergonomics, energy consumption, hazardous raw materials and so on [6]. Following in the footsteps of these two programmes, various corporate organisations and/or their IT divisions have taken measures aligned to the green computing notion to lower the effect of their IT operations on the environment [7].

3. Mining through Proof-of-Work

There are mainly two types of blockchains in terms of access type: permissionless (public) and permissioned (private). In a permissionless blockchain network any internet-enabled device can act as a participating node having write and read access to the chain of blocks i.e. the data. Per contra, in a permissioned blockchain ecosystem, participation is subject to permission - only certain nodes, as defined by the protocol code, have the privilege to write, while mostly all other permitted nodes have read access.

In a permissionless blockchain network, such as Bitcoin, a participating node willing to make a transaction has to trigger the transaction by broadcasting it to the network. Other participants of the network then verify and validate the transaction, following the rules set by the protocol. These verified and validated transactions are then gathered into a pool of "unconfirmed" transactions. All, or an asymmetric partial cohort, of the transactions are then combined into a "candidate" block by the participating nodes.

Along with other relevant information, a "coinbase" transaction and a nonce is then added before calculating the "hash" of the candidate block. Unlike ordinary transactions, a coinbase does not have an input transaction number/address (pointer) – this is a new transaction creating brand new coins, following the latest reward rate as defined by the protocol, with an output to the participating node competing to successfully generating the block. This thus works as an incentive to the competing node. Analogous to gold mining, this process is also known as (cryptocurrency) mining and the competing nodes are known as the miners.

To successfully release (or acquire) the newly created coins, for which the reward is 12.5 Bitcoins (BTC) as of March 2019, the calculated hash has to meet certain criteria i.e. the difficulty level. The difficulty level is a threshold: the calculated hash must be smaller than this threshold or in other words must start with a certain number of zeros. A brute force approach is adopted to calculate the hash meeting the threshold. This is achieved by repeating the hash calculations by changing the value of the nonce, usually increasing by one, until the threshold is met. Once the threshold is met, the block is then sealed and broadcasted to the network for consensus. Other nodes then verify the claim and, if satisfied, add it to their existing chain of blocks and start working on building a new candidate block. All the nodes thus have an updated copy of the chain.

The whole process is known as Proof-of-Work (PoW) as the miners have to "do" some work i.e. use their computing power and burn electric energy. Due to the increased demand and popularity, the price of Bitcoin and other cryptocurrencies has increased massively. This has resulted in increased participation in the mining process, making mining very competitive. As a result, the use of performance-enhanced devices such as Application-Specific Integrated Circuits (ASIC) has gained popularity. Formation of miners' pools has also become a norm where a cohort of miners works in a group to increase the chances of winning and the mining reward is shared. This trend is also pertinent in mining altcoins – cryptocurrencies other than Bitcoin.

The importance and necessity of PoW lies in the mutability, trust, security and transparency offered by blockchain - discussion of which is outside the scope of this paper.

4. Green Computing Vs. PoW Mining

Mining through the PoW consensus approach has put tremendous demand on the supply of energy in terms of electricity. Dwyer and Malone's study on Bitcoin's energy footprint reveals that the electricity consumed for mining in the Bitcoin network in 2014 was approximately equivalent to the total electricity consumed in Ireland during the same period of time [8]. In addition, the number of bitcoin transactions is ever increasing. Pantera Capital reported an average annual growth of the Bitcoin network by 110% between 2012 and 2016 [9]. This growth in transactions obviously results in a proportionately increased level of mining. Furthermore, with the passage of time, the size of Bitcoin blockchains steadily increases and this results in increased consumption of electricity, accordingly. In November 2017 Malmo [10] reported that on an average a single Bitcoin transaction consumes 215 KWh which is equivalent to average household electricity consumption in a week. In fact, the major contribution in this calculation comes from the many failed attempts at the PoW puzzle. While all the miners from around the globe compete the block, only one wins. As per the Digiconomist estimation, Bitcoin's electricity consumption is equivalent to a 0.23% share of the world's total electricity consumption as of 21 March 2019 [11] - this share has nearly doubled within last 1.5 years.

The aforementioned statistics are only for Bitcoin. In fact, there are many other altcoins such as Ethereum, Litecoin and so forth, all following similar PoW algorithms and mining concepts. Thus, cryptocurrency mining is evidently a major emerging source of carbon footprint.

Apart from energy consumption, electronic waste (E-waste) produced by mining is another major environmental concern. Mining encourages the use of performance-specific hardware, such as ASICs, which becomes obsolete in approximately every 1.5 years and contributes to, as of early 2021, the average e-waste generated by Bitcoin estimated at 64.4 metric kilotons per year [12]. Similar to electricity consumption, the E-waste generated by other altcoins also needs to be considered.

The aim of creation of Bitcoin was to shift the trust from financial intermediaries to the networks of participating nodes, with blockchain functioning as a "Trust Machine" [13]. Thus, Bitcoin and other altcoins are not backed by any sort of tangible assets. Therefore, such extreme strain on the environment, resulting from virtual currencies, is being highly criticised on environmental grounds.

In fact, the application of blockchain has now reached beyond cryptocurrencies [14]. Multifaceted applications, especially those offered by Ethereum and other similar blockchain technologies, has made smart-contracts, ICO's (Initial Coin Offering), DAOs (Decentralised Autonomous Organization) and DApps (Decentralised Apps) very popular [15]. These applications also contribute to higher mining rates.

Recent implementation of Lightning Network and other similar technologies allows transactions to take place in a second layer (also known as layer 2) – a separate layer than the base blockchain layer. Rather than every single transaction being recorded after successful completion of the consensus method, the final resultant balance is broadcast to the network at the time of exiting the channel. Therefore, this is likely to reduce the amount of consensus needed; however, the technology is still in its infancy and the future adoption trends are highly dependent on many other factors, including the level of security it can offer. That being said, consensus will still be required for verifying, validating and recording the resultant balance of the intermediate transactions [16].

5. Green Alternatives to PoW Mining

Developers and researchers have thus far proposed, designed and implemented a few other consensus algorithms for blockchain technology. Amongst them, the major ones are as follows:

Proof-of-Stake (PoS): After PoW, PoS has received the highest level of attention from developers and researchers. In contrast to an open completion as in PoW, the PoS approach deploys a selection method for granting sovereignty for the purpose of creating the next block. This is mainly based on the amount of coins or wealth (i.e. stake) a node possesses, in combination with other selection algorithms such as randomized block selection and coin age-based selection. While this is more eco-friendly, the higher the amount of stakes a node possesses, the higher are the chances of getting selected, creating a form of centralisation. Thus, this contradicts the decentralisation concept brought by blockchain. Peercoin is the first cryptocyrrency to use PoS. Ethereum's future roadmap of development includes a paradigm shift from PoW to PoS and is currently at the stage of experimenting with different variations of PoS.

Delegated Proof-of-Stake (DPoS): DPoS is basically another variation of PoS. However, it is worth mentioning as a separate category since it has recently gained vast attention and has been utilised in various projects [17]. DPoS deploys only a limited number of nodes with the authority to propose and validate blocks to be added to the existing chain of blocks. DPoS is proving to be fast due to a lower number of nodes being used for reaching consensus, compared to PoS and PoW. DPoS is, therefore, having a less negative impact on the environment.

Proof-of-Activity (PoA): PoA is a hybrid of both PoW and PoS[18]. It first uses PoW to determine a "miner" for creating the block, containing only the relevant head information and miner's address but no transactions. Once the PoW is achieved, PoA selects the signing nodes (validators) using PoS. Unlike PoW and PoS, transactions are then added to the block. Once the transactions are validated and the signed by the validators, it is added to the existing block. The mining rewards are proportionately shared by the PoW miner and PoS validators, based on their activities and role. Thus, similar to PoW, PoE also suffers a high demand of energy during the PoW phase. Furthermore, it possesses the same risk of centralisation as found in PoS.

Proof-of-Capacity (PoC): In PoC (also known as Proof of Space), the selection of miner is based on the amount of disk space filled with plots [19]. These plots are pre-recorded probable "nonce" values which are generated through iteration hashing of data. Analogous to PoS, the higher the amount of disk space plotted, the higher the chance of winning. However, in contrast to PoW, PoC is considered more environmentally friendly as it can be performed with regular computing resources without needing performance enhancing devises such as ASICs and the up-front computational cost of the plotting process is far less than solving a PoW puzzle. Furthermore, unlike PoW, miners can re-use their existing plots repeatedly, which reduces the running cost (consumption of power) and thus PoC not only makes mining eco-friendly but also economical.

There are a few other consensus algorithms such as Proof-of-Burn, Proof-of-Identity, Proof-of-Importance, Proof-of-Property, Proof-of-Approval, Transactions as Proof of Stake (TaPoS) and so on. While some of these are green in nature compared to PoW, they are mostly not a good fit for use in a permissionless blockchain such as Bitcoin and Ethereum. Most of them bring back centralisation, as opposed to decentralisation – the main purpose of introducing cryptocurrency. Thus, while they may outperform PoW in eco-friendliness, they are rather better suited for permissioned blockchains.

6. Concluding Discussions

The level of security, immutability, transparency and verifiability offered by permissionless blockchain is generated by the mathematical hashing, use of asymmetric encryption keys and PoW consensus approach. PoW also provides protection against a distributed denial of service (DDoS) attack [20] and double spending of the same cryptocurrency [13-14]. A DDoS attack, by capturing at least 51% of the total computing power within the network is not only highly expensive but also not risk free from a hacker's investment point of view. Hackers are highly likely to wind up spending more money than they can subterfuge. Therefore, PoW is essential to maintain the level of security and immutability offered by blockchain. However, this extra layer of security powered by PoW is achieved by trading off against a heavy cost with regard to environmental sustainability. Thus, it triggers an urgent need to design and develop better alternatives.

This paper briefly discussed how the PoW consensus approach works, exemplifying the way it has been utilised in Bitcoin's network. It has then surveyed how mining through PoW negatively contributes toward the notion of green computing. Finally, the paper briefly presents, compares and contrasts other alternative approaches being researched, some of which have a greener environmental footprint, but have counterbalancing disadvantages. Future research directions will include simulating various consensus approaches in terms of greenness and the level of security they can offer.

References

[1] EPA, "Sources of Greenhouse Gas Emissions", *Greenhouse Gas Emissions*, Available: https://www.epa.gov/ghgemissions/sources-greenhouse-gas-emissions.

[2] Mario Pickavet, Willem Vereecken, Sofie Demeyer, Pieter Audenaert, Brecht Vermeulen *et al.*, "Worldwide energy needs for ICT: the rise of power-aware networking", in *Proceedings of the 2nd International Symposium on Advanced Networks and Telecommunication Systems*, December 2008, DOI: 10.1109/ANTS.2008.4937762, Available: https://ieeexplore.ieee.org/document/4937762.

[3] Lotfi Belkhir and Ahmed Elmelig, "Assessing ICT global emissions footprint: Trends to 2040 & recommendations", *Journal of Cleaner Production*, Vol. 177, 2018, pp. 448-463, DOI: 10.1016/j.jclepro.2017.12.239, 2 January 2018, Available: https://www.sciencedirect.com/science/article/pii/S095965261733233X?.

[4] Savitha Chinnadurai and Kiran Nandavarapu, "Increasing Carbon Footprint of the ICT Sector", in *Course5 Transformative Intelligence*, 23 November 2015, Available: https://www.course5i.com/blogs/increasing-carbon-footprint-of-the-ict-sector-2/.

[5] Energy Star, "Energy Star Overview", Available: https://www.energystar.gov/about.

[6] TCO Certified, “The story of TCO Certified”, Available: https://tcocertified.com/the-story-of-tco-certified/.

[7] Brian Donnellan, Edward Curry, Bill Guyon and Charles Sheridan, “Developing a Sustainable IT Capability: Lessons From Intel’s Journey,” in *MIS Quarterly Executive*, vol. 11, no. 2, pp. 61–74, 2012, Available: https://aisel.aisnet.org/misqe/vol11/iss2/3.

[8] Karl J. O'Dwyert and David Malone, “Bitcoin Mining and its Energy Footprint”, in *Proceedings of the 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, DOI: 10.1049/cp.2014.0699, ISBN: 978-1-84919-924-7, 26-27 June 2014, Ireland, Available: https://digital-library.theiet.org/content/conferences/10.1049/cp.2014.0699.

[9] Pantera capital, “Bitcoin Continues Exponential Growth in 2016 :: Blockchain Letter, February 2017”, in *Medium*, 2 February 2017, Available: https://medium.com/@PanteraCapital/bitcoin-continues-exponential-growth-in-2016-blockchain-letter-february-2017-9445c7d9e5a2.

[10] Christopher Malmo, “One Bitcoin Transaction Consumes As Much Energy As Your House Uses in a Week”, in *Motherboard*, 1 November 2017, Available: https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change.

[11] Digiconomist, “Bitcoin Energy Consumption Index”, in *Digiconomist*, 21 November 2017, Available: https://digiconomist.net/bitcoin-energy-consumption.

[12] Alexde Vries and Christian Stoll, “Bitcoin's growing e-waste problem”, Resources, Conservation and Recycling, Vol. 175, 2021, p. 105901, Elsevier B.V., DOI: 10.1016/j.resconrec.2021.105901, Available: https://www.sciencedirect.com/science/article/pii/S0921344921005103?.

[13] Mahdi H. Miraz and Maaruf Ali, “Blockchain Enabled Enhanced IoT Ecosystem Security”, in *Proceedings of the International Conference on Emerging Technologies in Computing 2018 (iCETiC '18)*, 23-24 August 2018, London Metropolitan University, London, UK, Part of the Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol. 200, Online ISBN: 978-3-319-95450-9, Print ISBN: 978-3-319-95449-3, Series Print ISSN: 1867-8211, Series Online ISSN: 1867-822X, DOI: 10.1007/978-3-319-95450-9_3, pp. 38-46, Published by Springer-Verlag, available: https://link.springer.com/chapter/10.1007/978-3-319-95450-9_3.

[14] Mahdi H. Miraz and Maaruf Ali, "Applications of Blockchain Technology beyond Cryptocurrency” in *Annals of Emerging Technologies in Computing (AETiC)*, pp. 1-6, Vo2. 1, No. 1, 1st January 2018, Published by International Association of Educators and Researchers (IAER), Print ISSN: 2516-0281, Online ISSN: 2516-029X, DOI: 10.33166/AETiC.2018.01.001, Available: http://aetic.theiaer.org/archive/v2n1/p1.html.

[15] Mahdi H. Miraz and David C. Donald “Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities”, in *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 11-18, Vol. 3, No. 1, 1st January 2019, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2019.01.005, Available: http://aetic.theiaer.org/archive/v3/v3n1/p5.html.

[16] Mahdi H. Miraz and David C. Donald, “LApps: Technological, Legal and Market Potentials of Blockchain Lightning Network Applications”, in *proceedings of the 3rd International Conference on Information System and Data Mining (ICISDM2019)*, April 2019, University of Houston, USA, published by ACM, pp. 185–189, DOI: 10.1145/3325917.3325942, Available: https://dl.acm.org/doi/10.1145/3325917.3325942.

[17] Crypto Stella, "Explain Delegated Proof of Stake Like I'm 5" in *Hacker Noon*, 28 September 2017, Available: https://hackernoon.com/explain-delegated-proof-of-stake-like-im-5-888b2a74897d.

[18] Jake Frankenfield, “Proof of Activity (Cryptocurrency)”, in *Investopedia*, 4 April 2018, Available: https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp.

[19] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov and Krzysztof Pietrzak, “Proof of Space”, in *Advances in Cryptology -- CRYPTO 2015*, Part of Lecture Notes in Computer Science, Vol. 9216, pp. 585-605, DOI: 10.1007/978-3-662-48000-7_29, 01 August 2015, Available: https://link.springer.com/chapter/10.1007/978-3-662-48000-7_29.

[20] Ahmed S. Abu Daia, Rabie A. Ramadan and Magda B. Fayek, “Sensor Networks Attacks Classifications and Mitigation”, in *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 28-43, Vol. 2, No. 4, 1st October 2018, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2018.04.003, Available: http://aetic.theiaer.org/archive/v2/v2n4/p3.html.