



OPEN ACCESS

EDITED BY

Yizhong Liu,
Beihang University, China

REVIEWED BY

Yueyue Dai,
Huazhong University of Science and
Technology, China

*CORRESPONDENCE

Rameez Asif,
✉ rameez.asif@uea.ac.uk

RECEIVED 26 January 2023

ACCEPTED 17 August 2023

PUBLISHED 31 August 2023

CITATION

Asif R and Hassan SR (2023), Shaping the
future of Ethereum: exploring energy
consumption in Proof-of-Work and
Proof-of-Stake consensus.
Front. Blockchain 6:1151724.
doi: 10.3389/fbloc.2023.1151724

COPYRIGHT

© 2023 Asif and Hassan. This is an open-
access article distributed under the terms
of the [Creative Commons Attribution
License \(CC BY\)](#). The use, distribution or
reproduction in other forums is
permitted, provided the original author(s)
and the copyright owner(s) are credited
and that the original publication in this
journal is cited, in accordance with
accepted academic practice. No use,
distribution or reproduction is permitted
which does not comply with these terms.

Shaping the future of Ethereum: exploring energy consumption in Proof-of-Work and Proof-of- Stake consensus

Rameez Asif* and Syed Raheel Hassan

School of Computing Sciences, University of East Anglia, Norwich, United Kingdom

Ethereum (ETH) is a popular Layer-1 blockchain platform that has been used to create decentralized applications (dApps) and smart contracts. Ethereum 2.0, or Serenity, is a significant update to the network that intends to address numerous issues with scalability, security, and energy efficiency. The Proof-of-Stake (PoS) consensus method will replace the Proof-of-Work (PoW) mechanism, which is one of the major new features of Ethereum 2.0. Given that PoS doesn't require miners to do intensive mathematical calculations in order to validate transactions, it has the potential to be more energy-efficient than PoW. Additionally, this Ethereum upgrade will also be more secure due to the introduction of a new mechanism called "Casper" that will ensure that validators are always in agreement on the state of the blockchain. The paper begins by discussing the current issues facing Ethereum, including the limitations of the Proof of Work (PoW) consensus mechanism and the need for more efficient and scalable solutions. In this study, we peered at the major changes introduced by Ethereum 2.0, such as the new consensus method (Proof-of-Stake) and the addition of shard chains (Ethereum 2.0), as well as the associated development timelines, benefits and the community criticism on this upgrade.

KEYWORDS

blockchain, Ethereum, Bitcoin, cryptocurrencies, cybersecurity, cryptography, security, privacy

1 Introduction

Blockchain is a distributed, digital ledger that records network-wide transactions. It is the technology that underpins cryptocurrencies such as Bitcoin, but it has the potential to be utilised for a wide range of other applications (Ali Syed et al., 2019). A crucial characteristic of blockchain is its security and privacy. Security is a fundamental component of blockchain technology. The fact that each block in a blockchain contains a cryptographic hash of the preceding block as well as a timestamp makes it exceedingly difficult to alter the data contained in the blockchain. Furthermore, transactions on a blockchain network are validated by several nodes, making it even more difficult to modify or falsify data (Asif et al., 2021; Bhutta et al., 2021).

Additionally, privacy is a key component of blockchain technology. Only the members participate in a transaction may access the parameters of a blockchain transaction. Smart contracts may be used to establish private, permissioned blockchains that are only available to authorised parties, so enhancing privacy even further (Lin et al., 2021). One of the most potential applications of blockchain technology is supply chain management. Companies

may construct a transparent and tamper-proof record of the movement of products from the point of origin to the point of sale using blockchain technology (He et al., 2020). This may promote trust and eliminate fraud in supply chains, as well as increase efficiency and save costs. Using blockchain technology in voting systems to make the process more safe and transparent is another possible application (Wang et al., 2020).

Bitcoin and Ethereum, among others, rely on the underlying blockchain technology. It is the backbone of digital currency, ensuring safe and transparent exchanges that may operate independently of any one governing body (Watorek et al., 2021). Many people now consider cryptocurrencies as a legitimate kind of digital cash, and these tokens are being used for everything from online shopping to day trading. Digital currencies have also been bought and held as a sort of alternative investment by many people. Blockchain technology is central to cryptocurrencies, but its applications go well beyond money transfers (Sabry et al., 2020). Decentralized apps (dApps) built on the blockchain using blockchain based smart contracts can be employed in a broad variety of novel scenarios.

Bitcoin's enormous transactional, trust, and security advantages are offset by the actively resource-intensive design of its transaction verification process, which now compromises our ability to survive in a climate-dependent world (Truby, 2018). Indeed, Bitcoin mining and transactions are an application of Blockchain technology that makes inefficient use of scarce energy resources for a financial activity at a time in human development when world governments are scrambling to reduce energy consumption in accordance with their climate change commitments under the Paris Agreement and beyond to mitigate future climate change implications (Truby et al., 2022). Policies and frameworks are under-development but basic working technology of blockchain is still power hungry and adding the significant amount of carbon foot print. In the integration of blockchain, it is necessary to resolve multiple issues. While some protocols aim to increase blockchain throughput and reduce transaction confirmation latency, others aim to reduce PoW's energy consumption. Others concentrate on enhancing the security of the blockchain (Xu et al., 2023).

Proof-of-work (PoW) consensus algorithms, used by blockchains like Bitcoin, are very energy-intensive to administer and secure. Powerful computers solving complicated mathematical problems consume a lot of energy during the mining process required to validate transactions and add them to the blockchain (Ismail and Materwala, 2019). Bitcoin's energy usage in 2020 is predicted to reach roughly 121.36 TWh, or more than the total annual energy consumption of nations like Argentina and the Netherlands, according to the University of Cambridge's Centre for Alternative Finance (Schletz et al., 2020; Fernando and Saravannan, 2021). As more miners join the network in pursuit of rewards, the energy requirements of the Bitcoin network may rise, according to some research. This is due to the fact that an increase in the number of miners on a network results in an increase in the complexity of the mathematical problems that must be solved in order to authenticate transactions on the network.

Ethereum, the second biggest blockchain network in terms of market capitalization (Chen et al., 2020), is now undergoing a significant update known as Ethereum 2.0 or merge or "Serenity" which intends to increase the network's scalability, security, and

energy efficiency. This review will summarise the upgrade that will occur in phases, commencing with the transition from a proof-of-work consensus method to a proof-of-stake algorithm. This action is intended to significantly decrease the energy consumption of the Ethereum network. Additionally, Ethereum 2.0 aims to increase network scalability by employing a new technique known as shard chains, which enables the parallel processing of transactions. This update is anticipated to introduce numerous new opportunities to the Ethereum network by the end of the second quarter of 2023. In this review, we have discussed the specifics of this transformation. In addition, we discussed the cutting-edge consensus algorithms, time frame, technical features, implementation issues, and impediments that the Ethereum community faces in preparation for this major update.

2 Blockchain consensus algorithms

Proof-of-Work (PoW) is a method in which users, also known as miners, compete to solve a difficult mathematical challenge to add a new block to the blockchain. The first miner to solve the challenge is awarded a certain amount of bitcoin tokens. Mining is the process of solving the challenge, which needs a substantial amount of processing power (Lashkari and Musilek, 2021). This computational activity ensures network security by making it harder for a single miner or group of miners to seize control of the network. Nonetheless, mining may be quite energy-intensive because to the computational processing required.

In order to add a new block to the blockchain, Proof-of-Stake (PoS) is a technique in which users must demonstrate ownership of a particular number of cryptocurrency tokens. Users are selected to add a new block to the blockchain based on the quantity of tokens they own and the period of time they have held them. This procedure is known as "staking" In this method, the more tokens an individual holds, the more "weight" they have in the network, and the greater their likelihood of being selected to add a new block (Lashkari and Musilek, 2021). This is due to the fact that users with more tokens have a bigger "stake" in the network and are therefore more driven to keep its security.

One of the primary benefits of PoS is that it consumes less energy than PoW, as depicted in Figure 1. This is because it does not require computational effort and hence uses less energy to operate (Lashkari and Musilek, 2021). Furthermore, because users are picked to add a new block based on the quantity of tokens they own, any single miner or group of miners has a lower chance of seizing control of the network. This might result in a more decentralised network. Proof of Stake also has the advantage of being more adaptable than PoW. This is due to the fact that users can stake their tokens in a variety of methods, such as through a validator or a delegator. This provides for more network diversity and can assist to make the network more robust to assaults. There are other technologies available that are energy efficient like IOTA, Solana and Hedera etc., but the market capitalization and technological maturity of Ethereum is still on the top of the Layer-1 blockchains. In addition to Ethereum, we have alternatives such as Cardano, a blockchain platform that employs a PoS consensus mechanism. It seeks to provide a secure, scalable, and energy-efficient infrastructure. Stellar, a blockchain-based platform designed for quick and inexpensive transactions, is an additional well-established

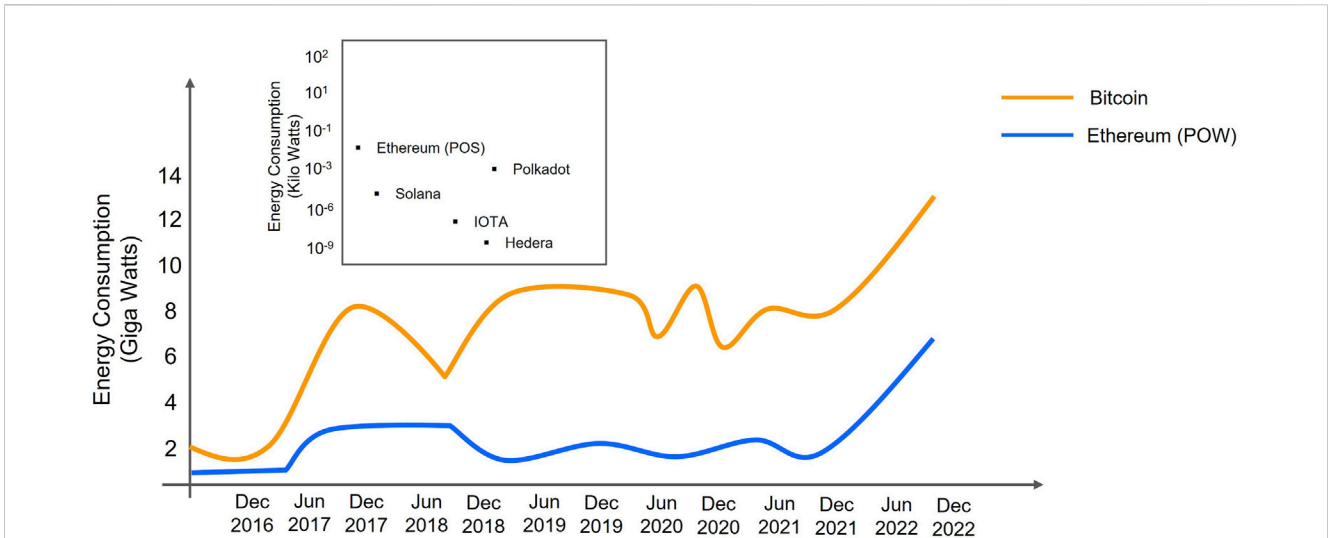


FIGURE 1 Energy consumption of Bitcoin, Ethereum based on proof-of-work (POW) and next generations of green Blockchains based on proof-of-stake (POS).

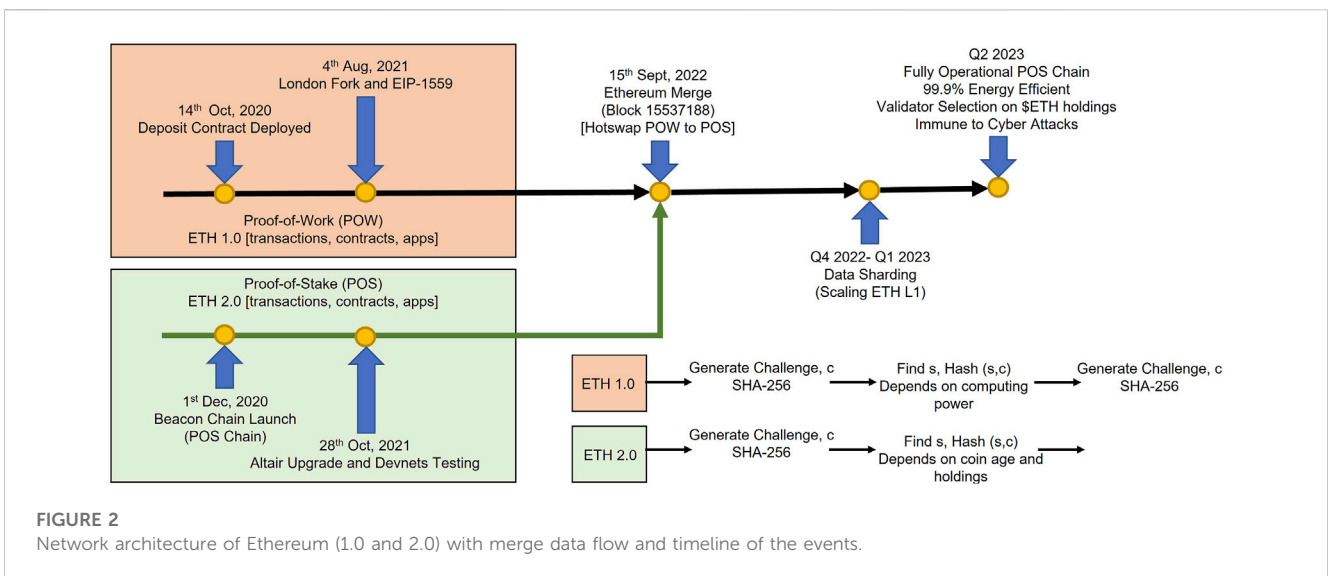


FIGURE 2 Network architecture of Ethereum (1.0 and 2.0) with merge data flow and timeline of the events.

framework. The Stellar Consensus Protocol (SCP), a federated Byzantine agreement algorithm, is utilised. SCP is considered more energy-efficient than PoW-based cryptocurrencies because it does not require energy-intensive mining. Nano is another framework that operates on the Block Lattice directed acyclic graph (DAG) structure. It employs a consensus mechanism based on delegated proof-of-stake (dPoS), which negates the need for miners. Representatives selected by coin holders conduct nano-transactions, resulting in minimal energy consumption.

3 Ethereum merge 2022

The fundamental reason for making the switch from PoW to PoS is to address several long-term scalability and sustainability

problems with the present PoW consensus process, which Ethereum has been using up until now. PoS outperforms PoW in several ways, including energy efficiency, scalability, security, and cost (Cao et al., 2020). Additionally, PoS is more acceptable to a wider audience because it does not need sophisticated and expensive infrastructure. The Ethereum community has been planning the switch from PoW to PoS for quite some time, and much effort is being put in to making the changeover as painless as possible for everyone involved: users, developers, and miners (Lepore et al., 2020). Being up-to-date on developments and innovations in the blockchain and PoS space is crucial for researchers and practitioners, as depicted in Figure 2. The exact timeline for this Ethereum undergone several changes, but the current plan is as follows:

- **Phase 0 (Beacon Chain):** The Beacon Chain is the first phase of the Ethereum 2.0 upgrade, which went live on 1 December 2020. It introduces a new PoS-based chain that will eventually serve as the foundation for the rest of the Ethereum 2.0 upgrade. This phase introduces the concept of “validators” who will be responsible for validating transactions and creating new blocks on the network. These validators are chosen based on the amount of Ether they are willing to “stake” as collateral. The Beacon Chain also includes a mechanism for “shuffling” validators to prevent centralization and to ensure that the network remains decentralized.
- **Phase 1 (Shard Chains):** This phase is planned to introduce the shard chains, which is a scaling solution for Ethereum 2.0 and will allow the network to process more transactions in parallel. Shard chains are smaller sub-networks that can process transactions independently, but still maintain the same level of security as the main chain. This phase will introduce 64 shard chains, which will greatly increase the network’s overall capacity and allow for more complex and resource-intensive dApps to be built on the Ethereum network.
- **Phase 1.5 (Merge Phase):** This phase will consist of merging the current Ethereum PoW chain with the Beacon Chain, which will allow the existing Ethereum network to operate on top of the new PoS chain. This phase will be a critical step in the transition from PoW to PoS and will ensure a smooth transition for users, developers, and miners.
- **Phase 2 (Execution Environments):** This phase will introduce new virtual machines that will allow for more advanced smart contract execution and more efficient data storage. This phase will introduce new features such as “eWASM” (Ethereum-flavored WebAssembly) which will allow for more efficient and powerful smart contract execution, as well as new data structures such as “light clients” which will allow for more efficient data storage.

It is important to note that modifications often involve making substantial adjustments to the blockchain network’s underlying technology, which may be both complicated and time-consuming. In addition, the upgrading process might be interrupted or delayed if bugs or other technical difficulties develop. Another potential stumbling block to the upgrading process is user acceptance of the new consensus method and other network modifications (Pang, 2020). It can cause people to stop contributing, which in turn makes the network less secure. Potential security flaws in the upgraded network’s new consensus mechanism or elsewhere in the system are only one example of the dangers that might arise as a result of the upgrading process. There is also the possibility that malicious actors will seek to use these flaws to take over the network.

4 Current research updates

In this section, we have discussed active PoS related research and development efforts. Various teams in the blockchain community are developing and researching many new initiatives. The blockchain and PoS fields are constantly evolving, and it is

critical for practitioners and academics to remain up-to-date on the latest advancements and breakthroughs. These research advancements include not only the creation of adaptive PoS algorithms, but also the effective utilisation of network resources, i.e., sharding (Liu et al., 2021). These research activities will be summarised below.

Adaptive Proof of Stake (APoS) is a proposed consensus mechanism that seeks to improve on conventional PoS systems by dynamically adapting the difficulty of block validation based on network conditions. This is meant to improve system efficiency and security by minimising the possibility for centralization and expanding the network’s validators (Gaži et al., 2019). Sharding is a scalability option for blockchains that allows the network to be divided into smaller sub-networks that can run in parallel. PoS is seen to be a suitable fit for sharding because it improves system security and scalability by distributing the validation process over multiple validators (Yu et al., 2020). Researchers are investigating how to utilise PoS to safeguard sharded blockchain systems, including cross-shard communication and the use of economic incentives to guarantee system security.

Staking pools and validator services let users to engage in PoS networks and receive incentives for staking their cryptocurrencies more effectively. Researchers are looking at ways to make these pools and services more secure and decentralised by offering new methods of selecting validators and increasing incentives for users to stake their currencies (Kim et al., 2021). Researchers are also looking at ways to make PoS networks more secure and resistant to assaults, such as detecting and addressing potential vulnerabilities in the consensus mechanism. This involves researching possible attack vectors and developing new security measures to defend against them, such as new cryptographic algorithms to encrypt network communication and transactions.

5 Challenges and criticism on PoS

Following the successful first-phase update of the Ethereum network, the community has had conflicting views to the new consensus method. One of PoS’s greatest strengths is that it uses energy very efficiently. According to the Ethereum Foundation, the current Proof-of-Work system consumes roughly 5.13 gigawatts on a continuous basis, whereas the Proof-of-Stake system consumes only 2.62 MW, or about 99.95% less energy. The main criticisms of the Ethereum PoS upgrade include concerns about centralization, as a small number of large stakeholders, known as “whales,” may hold a disproportionate amount of the network’s validating power. Additionally, some critics argue lack of security, incentives and fairness. Some the challenges and arguments are discussed as:

- **Centralization:** One of the main criticisms of PoS is that it can lead to centralization, as users with more tokens will have a greater influence on the network. This can result in a small group of users controlling the majority of the tokens and therefore, the majority of the power in the network.
- **Wealth Concentration:** PoS can also lead to wealth concentration, as users who can afford to buy and hold a large number of tokens will have a greater influence on the network. This can result in a small group of wealthy users

controlling the majority of the network and making it less accessible to average users.

- **Security Concerns:** Critics argue that PoS systems are less secure than Proof of Work (POW) systems, as it is possible for a group of users with a large amount of tokens to collude and gain control of the network, making it more vulnerable to attacks.
- **Lack of Incentives:** PoS systems can lack incentives for users to validate transactions and secure the network, as they are not rewarded for doing so. This can result in a lower level of security and stability in the network.
- **Complexity:** PoS systems can be more complex than POW systems, which can make it difficult for average users to understand and participate in the network.
- **Lack of Fairness:** Critics argue that PoS systems can be unfair as it favors the ones that already have a significant amount of coins, making it harder for new users to participate.

6 Future research directions

There are several areas of research that can be explored to further improve PoS algorithms and address any potential limitations. One area of research could focus on optimizing PoS algorithms to improve their security and decentralization properties while also reducing energy consumption (Gupta et al., 2019). Another area of research could investigate the scalability limitations of PoS algorithms and explore ways to address them (Pang, 2020). Additionally, research could be conducted on how to mitigate the risk of centralization in PoS algorithms and ensure a fair distribution of validating power among network participants. Another important area of research is to investigate the performance of PoS consensus algorithms in the presence of malicious actors and measures to prevent Sybil attacks. In addition to technical aspects, there could be research on the governance and decision-making implications of PoS consensus algorithms. Furthermore, research could be done on how to integrate PoS algorithms with other emerging technologies such as smart contracts and decentralized finance

References

- Ali Syed, T., Alzahrani, A., Jan, S., Siddiqui, M. S., Nadeem, A., and Alghamdi, T. (2019). A comparative analysis of blockchain architecture and its applications: problems and recommendations. *IEEE Access* 7, 176838–176869. doi:10.1109/ACCESS.2019.2957660
- Asif, R., Ghanem, K., and Irvine, J. (2021). Proof-of-puf enabled blockchain: concurrent data and device security for internet-of-energy. *Sensors* 21, 28. doi:10.3390/s21010028
- Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., et al. (2021). A survey on blockchain technology: evolution, architecture and security. *IEEE Access* 9, 61048–61073. doi:10.1109/ACCESS.2021.3072849
- Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M., et al. (2020). Performance analysis and comparison of pow, pos and dag based blockchains. *Digital Commun. Netw.* 6, 480–485. doi:10.1016/j.dcan.2019.12.001
- Chen, H., Pendleton, M., Njilla, L., and Xu, S. (2020). A survey on ethereum systems security: vulnerabilities, attacks, and defenses. *ACM Comput. Surv.* 53, 1–43. doi:10.1145/3391195
- Fernando, Y., and Saravanan, R. (2021). Blockchain technology: energy efficiency and ethical compliance. *J. Gov. Integr.* 4, 88–95. doi:10.15282/jgi.4.2.2021.5872
- Gaži, P., Kiayias, A., and Zindros, D. (2019). “Proof-of-stake sidechains,” in 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019 (IEEE), 139–156. doi:10.1109/SP.2019.00040
- Gupta, K. D., Rahman, A., Poudyal, S., Huda, M. N., and Mahmud, M. A. P. (2019). “A hybrid pow-pos implementation against 51 percent attack in cryptocurrency system,” in 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Sydney, NSW, Australia, 11–13 December 2019 (IEEE), 396–403. doi:10.1109/CloudCom.2019.00068
- He, G., Su, W., Gao, S., and Yue, J. (2020). Td-root: a trustworthy decentralized dns root management architecture based on permissioned blockchain. *Future Gener. Comput. Syst.* 102, 912–924. doi:10.1016/j.future.2019.09.037
- Ismail, L., and Materwala, H. (2019). Article A review of blockchain architecture and consensus protocols: use cases, challenges, and solutions. *Symmetry* 11, 1198. doi:10.3390/sym11101198
- Kim, H. M., Laskowski, M., Zargham, M., Turesson, H., Barlin, M., and Kabanov, D. (2021). Token economics in real life: cryptocurrency and incentives design for insolar’s blockchain network. *Computer* 54, 70–80. doi:10.1109/MC.2020.2996572
- Lashkari, B., and Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. *IEEE Access* 9, 43620–43652. doi:10.1109/ACCESS.2021.3065880
- Lepore, C., Ceria, M., Visconti, A., Rao, U. P., Shah, K. A., and Zanolini, L. (2020). A survey on blockchain consensus with a performance comparison of pow, pos and pure pos. *Mathematics* 8, 1782. doi:10.3390/math8101782

(DeFi) to create new use cases and applications, such as supply chain management, finance and banking, voting and governance, intellectual property protection, gaming and digital assets and identity management etc. The effects of PoS consensus algorithms on the economy and the environment might also be studied.

Author contributions

RA and SH contributed to study the data. RA compiled the data, RA and SH compiled results and wrote the manuscript. RA and SH reviewed the paper for submission. All authors contributed to the article and approved the submitted version.

Acknowledgments

The authors like to acknowledge the regular updates from Vitalik Buterin on Ethereum Merge. Also special thanks to Digiconomist portal for keeping the energy consumption data open source.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher’s note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

- Lin, C., He, D., Huang, X., Xie, X., and Choo, K.-K. R. (2021). Ppchain: a privacy-preserving permissioned blockchain architecture for cryptocurrency and other regulated applications. *IEEE Syst. J.* 15, 4367–4378. doi:10.1109/JYST.2020.3019923
- Liu, C., Zhang, X., Chai, K. K., Loo, J., and Chen, Y. (2021). A survey on blockchain-enabled smart grids: advances, applications and challenges. *IET Smart Cities* 3, 56–78. doi:10.1049/smc2.12010
- Pang, Y. (2020). A new consensus protocol for blockchain interoperability architecture. *IEEE Access* 8, 153719–153730. doi:10.1109/ACCESS.2020.3017549
- Sabry, F., Labda, W., Erbad, A., and Malluhi, Q. (2020). Cryptocurrencies and artificial intelligence: challenges and opportunities. *IEEE Access* 8, 175840–175858. doi:10.1109/ACCESS.2020.3025211
- Schletz, M., Cardoso, A., Prata Dias, G., and Salomo, S. (2020). How can blockchain technology accelerate energy efficiency interventions? a use case comparison. *Energies* 13, 5869. doi:10.3390/en13225869
- Truby, J., Brown, R. D., Dahdal, A., and Ibrahim, I. (2022). Blockchain, climate damage, and death: policy interventions to reduce the carbon emissions, mortality, and net-zero implications of non-fungible tokens and bitcoin. *Energy Res. Soc. Sci.* 88, 102499. doi:10.1016/j.erss.2022.102499
- Truby, J. (2018). Decarbonizing bitcoin: law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies. *Energy Res. Soc. Sci.* 44, 399–410. doi:10.1016/j.erss.2018.06.009
- Wang, Y., Li, J., Zhao, S., and Yu, F. (2020). Hybridchain: a novel architecture for confidentiality-preserving and performant permissioned blockchain using trusted execution environment. *IEEE Access* 8, 190652–190662. doi:10.1109/ACCESS.2020.3031889
- Watorek, M., Drożdż, S., Kwapien, J., Minati, L., Oświecimka, P., and Stanuszek, M. (2021). Multiscale characteristics of the emerging global cryptocurrency market. *Phys. Rep.* 901, 1–82. doi:10.1016/j.physrep.2020.10.005
- Xu, J., Wang, C., and Jia, X. (2023). A survey of blockchain consensus protocols. *ACM Comput. Surv.* 55, 1–35. doi:10.1145/3579845
- Yu, G., Wang, X., Yu, K., Ni, W., Zhang, J. A., and Liu, R. P. (2020). Survey: sharding in blockchains. *IEEE Access* 8, 14155–14181. doi:10.1109/ACCESS.2020.2965147