MiCA Crypto Alliance

Environmental Impact of **ASIC-Resistant Coins**

Comparing the environmental costs of ASIC-resistant vs. ASIC-compatible PoW coins—energy, emissions, and decentralisation trade-offs.

In collaboration with Nodiens

Index

Highlights

01 ASIC mining is several orders of magnitude more energy- and carbon-efficient per unit of computational work, while ASIC-resistant mining prioritises a concept of decentralisation and accessibility using general-purpose hardware like GPUs and CPUs.

02 When measured per transaction, ASIC-resistant networks show lower energy use and emissions suggesting better efficiency for smaller-scale, user-driven systems.

03 ASICs offer higher hash rate security but contribute to mining centralisation. In contrast, ASIC resistance fosters wider participation but yields lower hash power, making networks potentially more vulnerable to attacks.

04 The trade-off between decentralisation and environmental efficiency defines the core dilemma of ASIC resistance in sustainable blockchain design.

Introduction

Proof-of-Work (PoW) is a widely adopted consensus mechanism that underpins several leading blockchain networks. By requiring computational work from miners, PoW secures transactions, ensures decentralisation, and maintains network integrity. However, this security comes at the (deliberate) cost of significant energy consumption. To optimise mining profitability, specialised hardware called Application-Specific Integrated Circuits (ASICs) have been developed, capable of performing hashing operations at unmatched speed and efficiency.

In response to the centralising tendencies of ASIC mining—where only those with access to the most advanced and expensive hardware can compete—some blockchain networks have implemented ASIC-resistant algorithms. These networks favor general-purpose hardware like GPUs and CPUs, aiming to democratise the mining process (Kuznetsov et al., 2023). Examples of some leading GPUs are Nvidia RTX 3090, Nvidia RTX 3080Ti and CPUs are AMD Ryzen 9 5950X, AMD Ryzen 9 7950X.

While the decentralisation benefits of ASIC resistance are clear, the environmental costs require careful examination. This report analyses the contrast between ASIC-resistant and ASIC-compatible PoW coins, with a focus on energy consumption, greenhouse gas emissions, and waste generation. These aspects may play an important role in portfolio management, especially when the asset management is intended to be sustainable and consider environmental impact.

ASIC Mining: High Efficiency, Low Flexibility

ASICs are custom-designed chips created to perform a very specific task — in the context of cryptocurrency, that task is mining a specific hashing algorithm extremely efficiently (Dutta et al., 2022). ASIC miners or rigs (often called ASICs themselves) are vastly more powerful than general-purpose hardware like CPUs or GPUs because they are optimised for only one type of operation.

For example, Bitcoin uses the SHA-256 hashing algorithm. An ASIC designed to mine Bitcoin will be useless for anything other than solving SHA-256 puzzles. But in doing so, it is many orders of magnitude faster and more energy-efficient than traditional hardware for its intended purpose. This level of efficiency means that, once ASICs are introduced for a particular algorithm, they quickly dominate the mining landscape for that coin.

Advantages of ASIC Mining:

- High Efficiency: ASICs tend to consume much less energy per hash (Crypto Analyst, 2024), but much more per rig as compared to GPUs or CPUs.
- Profitability: ASICs' lower energy intensity per hash means they generate a larger amount of dollars per kWh of energy consumption, which makes them more profitable than CPUs or GPUs.
- Network Security: ASICs contribute massive hashrates, making the network harder to attack (51% attack becomes expensive) (Aponte-Novoa et al., 2021).

Disadvantages of ASIC Mining:

- Centralisation: ASICs are expensive and primarily manufactured by a few companies, which can lead to centralised control over mining power. While it's true that GPUs are also predominantly produced by two major manufacturers, Nvidia and AMD, who together control over 90% of the discrete GPU market, the key difference lies in usage and ownership patterns. GPUs are general-purpose hardware used across a wide range of industries and applications (e.g., gaming, AI, graphics rendering), making them more widely distributed and accessible. In contrast, ASICs are designed for a single purpose of cryptocurrency mining, and their value is tied almost exclusively to that niche. This specificity limits their distribution and creates greater barriers to entry, increasing the risk of mining centralisation in the hands of a few well-funded entities.
- Lack of Flexibility: Most ASIC specialise in mining one algorithm only. If the coin changes algorithms or becomes unprofitable, the hardware becomes obsolete (Crypto Analyst, 2024).
- Barriers to Entry: ASIC mining is only profitable with access to cheap electricity, and because ASICs are designed to run at scale for maximum efficiency, they typically require wholesale energy prices and infrastructure, conditions out of reach for the average user (Cambridge Centre for Alternative Finance, 2024). This creates a high barrier to entry, reducing decentralisation in at least one of its dimensions (number of users with influence over the mining process).

ASIC-Resistant Mining: Democratising Access?

ASIC-resistant coins are cryptocurrencies designed to make mining with ASICs either technically difficult or economically unviable. These coins often rely on memory-hard algorithms, which fundamentally alter the nature of computation in a way that undermines the main advantage of ASICs: their ability to execute a specific, predictable computation at extremely high speed and low energy cost (Bertrand, 2022).

ASICs are designed to execute specific algorithms in a fixed, optimised manner using hardwired logic. ASICs are most efficient when:

- High Efficiency: ASICs tend to consume much less energy per hash (Crypto Analyst, 2024), but much more per rig as compared to GPUs or CPUs.
- Profitability: ASICs' lower energy intensity per hash means they generate a larger amount of dollars per kWh of energy consumption, which makes them more profitable than CPUs or GPUs.
- Network Security: ASICs contribute massive hashrates, making the network harder to attack (51% attack becomes expensive) (Aponte-Novoa et al., 2021).

This allows designers to hardwire the entire process with minimal control logic, achieving maximal speed and energy efficiency.

Hashing algorithms like SHA-256 (used in Bitcoin) are well suited to ASICs because they involve fast, repetitive operations with small, fixed memory needs. Instead, memory-hard algorithms, such as Equihash and RandomX, are engineered to do the opposite. They deliberately introduce characteristics that are antithetical to ASIC-friendly design:

- Large-capacity memory (several hundred megabytes to gigabytes)
- Random memory access patterns, making caching ineffective
- High bandwidth requirements to access memory quickly and frequently

Algorithms that introduce randomness or variability deliberately:

- Use data-dependent branching (e.g., the next operation depends on previous outputs).
- Involve non-deterministic control flow, meaning the execution path changes frequently based on intermediate results.

This breaks the regularity ASICs depend on. Implementing such behaviour in hardware requires:

- More control logic and hence large-capacity memory (several hundred megabytes to gigabytes)
- Random memory access patterns, making caching ineffective
- Requires high bandwidth to access memory quickly and frequently

all of which are features of CPUs or GPUs, not ASICs.

Because of this unpredictability, ASICs can't be optimised to the same degree:

- Much of their hardware sits idle while waiting on memory or conditional logic.
- Designing circuits to accommodate all potential code paths is costly in the silicon area.
- Power efficiency drops because more logic is needed per unit of useful computation.

As a result, the performance gap between ASICs and general-purpose processors narrows, making ASIC mining economically less attractive.

- Cost: Embedding large, fast memory (such as SRAM or DRAM) directly on an ASIC chip is prohibitively expensive in terms of die size and fabrication cost. Using off-chip memory increases latency and energy use, undermining ASIC performance and cost-efficiency.
- Design complexity: Random or data-dependent access patterns mean the logic must constantly fetch data from unpredictable locations. This is fundamentally different from the streamlined, pipelined computations ASICs are designed for.

General-purpose hardware—like CPUs and GPUs—is much better suited to these conditions since they are already equipped with:

- Large amounts of RAM
- Sophisticated memory controllers
- Caching strategies and branch prediction for handling irregular memory access

Therefore, memory-hard algorithms are much more efficiently executed on general-purpose hardware than on ASICs and used in ASIC resistant coins.

ASIC Resistant coins also helps to promote decentralisation in the following ways:

- Wider hardware access: General-purpose hardware is mass-produced, affordable and easily available to consumers worldwide. This lowers the entry barrier for individual miners and discourages monopoly control over mining hardware.
- Decentralised mining power: Since more people can mine using general purpose hardwares, the hashpower is distributed among a broader and more diverse group of participants, reducing the risk of a few entities dominating the network.
- Geographic diversity: ASIC-resistant mining does not require industrial-scale infrastructure, enabling smaller operations to exist in various locations, including urban and rural environments. This spreads the mining footprint across different jurisdictions and power grids, increasing the resilience of the network.
- Hardware reusability and exit options: In the event that mining becomes permanently unprofitable, CPUs and GPUs can be repurposed for other applications, unlike ASICs which become electronic waste. This flexibility attracts more participants who aren't locked into a single-purpose investment.

In essence, ASIC resistance shifts mining power from specialised industrial operators to a broader base of individual participants. Some notable ASIC-resistant PoW coins are Ethereum Classic (ETC), Monero (XMR), Kaspa (KAS), Ravencoin (RVN), Ergo (ERG), Ziliqa (ZIL).

Disadvantages of ASIC-Resistant Mining:

- More energy intensity: ASIC machines being designed for specialised operations are more energy efficient as compared to CPUs and GPUs which are more general purpose hardwares.
- Lower hashrate security: These networks tend to be smaller in hash rate terms (due to the lower hash rate per individual rig) and are more vulnerable to 51% attacks (Cho, 2018) because anyone with access to enough general-purpose hardware, which can be rented from cloud providers or bought easily or can potentially launch a 51% attack and make the network vulnerable to temporary control shifts.
- Software Complexity: To remain ASIC-resistant, these networks often need to change or tweak their algorithms regularly, which can complicate maintenance and user participation. This is done in an ad-hoc manner by scheduling hard forks every few months for example in Monero (Yap, 2018). Conversely, ASIC mined algorithms remain unchanged for years to ensure network stability and hardware longevity and allows for a more predictable development environment. They only see protocol level adjustments like difficulty adjustment, block time or block size changes that don't change the hashing algorithm itself but only adjust the mining landscape.

Methodology

This report employs a comparative analysis approach to evaluate the environmental impact of ASIC-compatible versus ASIC-resistant PoW coins. The primary source of all the metrics used in this study is Nodiens. The dataset includes information on hashrate, energy consumption, transaction counts, carbon emissions, and e-waste associated with a range of PoW crypto assets across both ASIC and ASIC-resistant mining ecosystems.

Energy consumption estimates are derived by analysing the network hashrate in conjunction with the profitability of mining each coin using a basket of profitable rigs released to the market at each moment in time. For comparability reasons, rig profitability is estimated by appeal to a uniform electricity price. This may understate the efficiency of ASIC-compatible networks versus ASIC-resistant ones, and future work in the field should incorporate energy price differences in this step. Once a basket of rigs such as ASICs, GPUs, or CPUs is established, their hash rate and power demand are taken to determine the average energy intensity per hash.

E-waste generation is calculated based on the basket of rigs that are actively used to operate nodes. The methodology accounts for the physical specifications of the hardware, particularly device weight, and applies depreciation rates—either technical or economic, depending on which occurs first—to estimate when the equipment becomes obsolete. This allows for a realistic approximation of the amount of mining hardware discarded each year.

Carbon emissions are estimated based on the energy mixes used by the miners, approximated by geographic distribution for on-grid mining nodes. By identifying the physical locations of mining activity, the model applies localised carbon intensity factors specific to those regions. This ensures an accurate representation of the climate impact of mining, which can vary widely depending on local energy sources and grid composition. Off-grid mining is identified manually and their energy sources are computed separately.

Results

To enable a standardised comparison, all the data for the year 2024 was annualised and normalised to calculate environmental impact per trillion units of computational work or terahashes (Th) and per transaction (tx). The following derived metrics were computed:

- Energy intensity (kWh/Th and kWh/tx): Calculated by dividing total energy consumption by total hashrate or transaction count, respectively.
- Carbon intensity (gCO_2e/Th and gCO_2e/transaction): Calculated by dividing total carbon emissions by total hashrate or transaction count.
- Waste Electrical and Electronic Equipment (WEEE) intensity (g/Th and g/tx): Calculated by dividing total e-waste generation by total hashrate or transaction count.

These calculations provide insight into the relative efficiency and environmental burden of ASIC-compatible and ASIC-resistant networks for the year 2024.

Using data from Nodiens, we compared the environmental impact of ASIC-mined coins (such as Bitcoin) and ASIC-resistant coins (such as Monero or Ravencoin). The results reveal a nuanced picture with significant trade-offs between the two categories.

	ASIC Mined Coins (Mean)	ASIC Resistant Coins (Mean)
Energy Consumption (kWh per Th)	0.007	25.143
Carbon Intensity (g per Th)	2.454	9,947.256
WEEE Intensity (g per Th)	0.003	41.935

When looking at the environmental cost per unit of computational effort (fig. 1), measured in terahashes (Th), ASIC-resistant coins appear dramatically less efficient. They consume energy that is higher in orders of magnitude and hence are more carbon intensive than ASIC mined coins. Similarly, they are way more waste intensive as compared to ASIC mined coins.

	ASIC Mined Coins (Mean)	ASIC Resistant Coins (Mean)
Energy Consumption (kWh per Tx)	734.25	340.50
Carbon Intensity (g per Tx)	247,459.57	124,091.11
WEEE Intensity (g per Tx)	134.00	318.44

When looking at the environmental cost per transaction (fig. 2), the picture becomes more nuanced. ASIC-resistant coins actually consume less energy and produce lower carbon emissions per transaction compared to ASIC-mined coins, although they are in the same order of magnitude. However, they generate more electronic waste per transaction, due to lower throughput in these networks, which may be attributed to the lower block size of ASIC-resistant networks and possibly lagging adoption. This highlights a trade-off, while ASIC-resistant networks may be cleaner in terms of energy and emissions per transaction, they are more waste-intensive.

Additionally, in the case of ASIC-mined coins, a significant portion of mining activity takes place off-grid, often in remote areas where miners can access low-cost, renewable energy sources such as hydro, wind, or solar power. These locations are chosen specifically for their energy affordability and availability, not necessarily their proximity to urban infrastructure. As a result, ASIC mining operations tend to have a higher share of renewable energy usage compared to ASIC-resistant mining, which is more commonly conducted on-grid using consumer hardware in residential or commercial settings.

While it's technically possible to mine with GPUs using off-grid renewable energy, in practice it's far less common and significantly less efficient than with ASICs. This is primarily because ASICs are purpose-built for mining and offer far higher performance per watt of energy consumed. Their efficiency makes them well-suited for deployment in off-grid, industrial-scale operations where maximising output from limited or variable renewable energy sources is crucial. GPUs, on the other hand, are general-purpose devices that are far less energy-efficient for mining. To achieve comparable output, a GPU mining setup would require far more hardware, more physical space, and more infrastructure—making it less cost-effective and harder to scale in remote, off-grid environments. Additionally, the small-scale plug-and-play nature of GPU mining makes it more accessible to individuals running rigs on conventional grid power at home or in urban areas. This is a key reason why ASIC mining is more often powered by renewables, while GPU mining typically draws from more carbon-intensive grids.

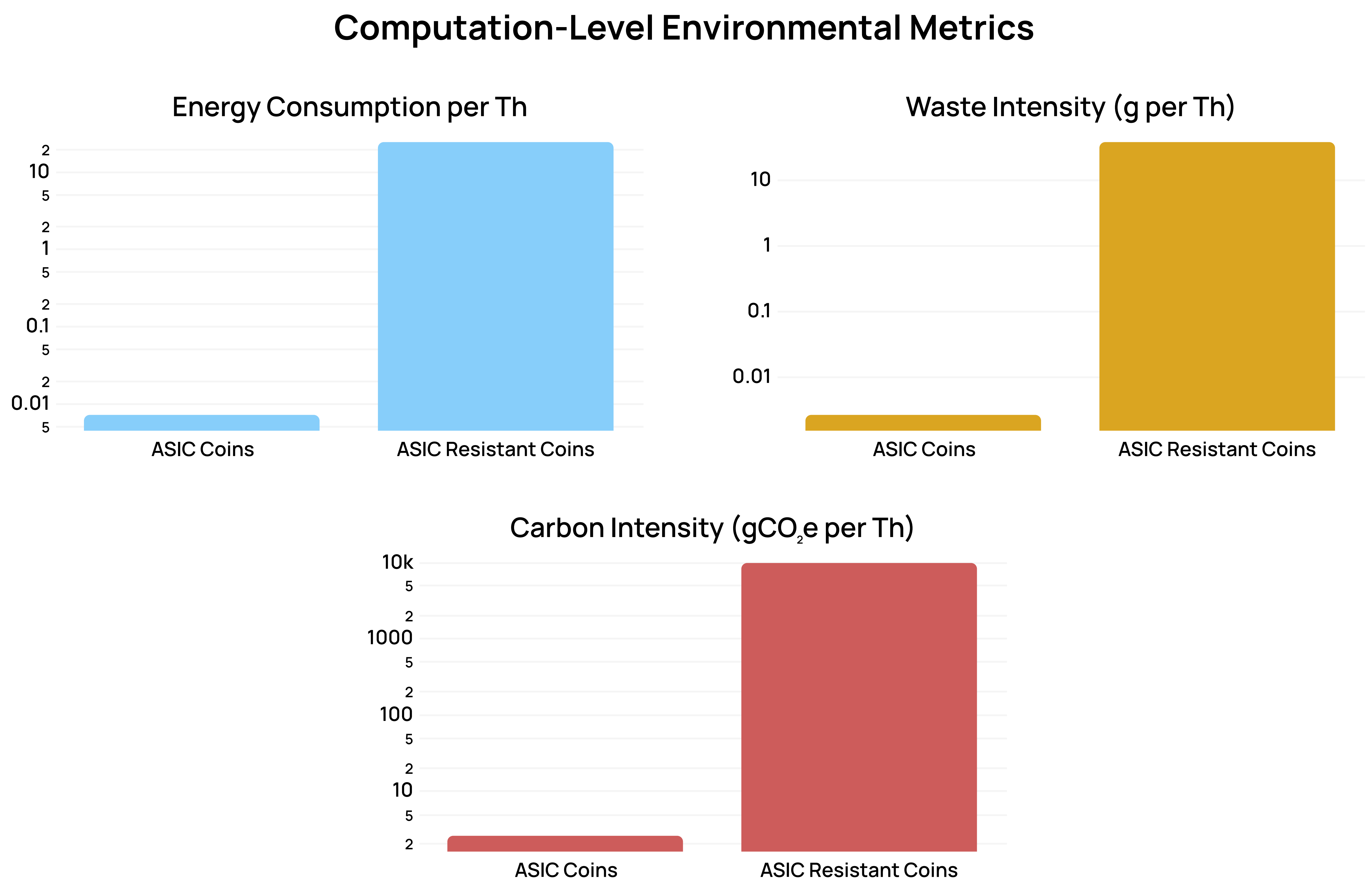

Figure 1: Environmental Cost of ASIC vs. ASIC Resistant Coins per unit of Computational Effort (Th).

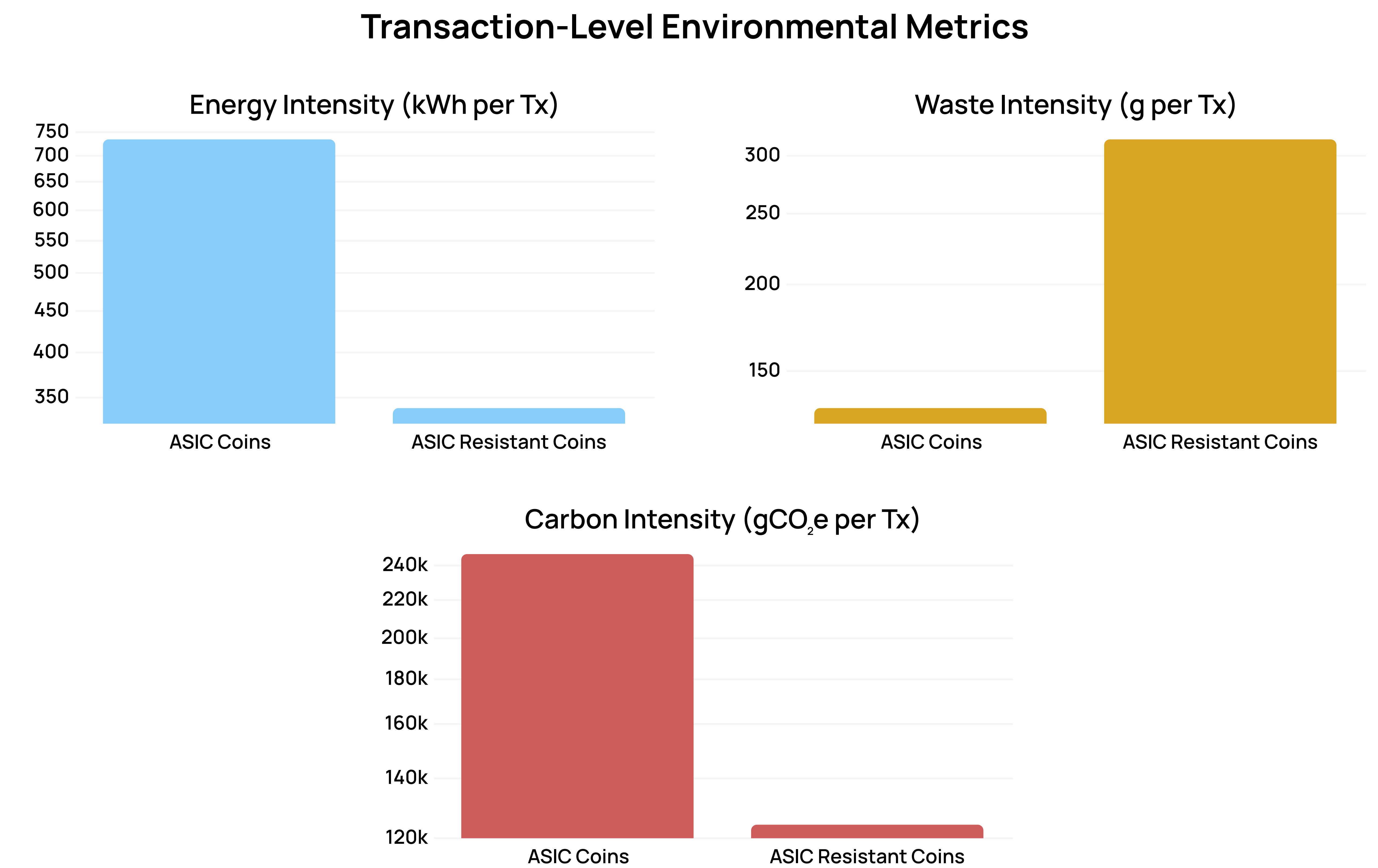

Figure 2: Environmental Cost of ASIC vs. ASIC Resistant Coins per Transaction.

Conclusion

This report set out to explore the environmental trade-offs between ASIC-mined and ASIC-resistant PoW cryptocurrencies. While ASIC resistance is often promoted as a way to decentralise mining and democratise participation, the environmental costs associated with this model raise important concerns.

Our analysis shows that ASIC mined coins are significantly more efficient in terms of energy use, carbon emissions, and e-waste generation per unit of computational work. This is largely due to their highly optimised, purpose-built nature, which allows them to achieve maximum performance with minimal energy input. Moreover, ASIC mining operations are more likely to be powered by off-grid renewable energy, further reducing their carbon footprint.

In contrast, ASIC-resistant coins - while more inclusive and accessible, suffer from substantially higher environmental overheads in terms of computational effort. They consume orders of magnitude more energy per terahash than ASIC-mined coins and generate exponentially more electronic waste per terahash, primarily due to the frequent turnover of general-purpose hardware such as GPUs and CPUs. However, when measured per transaction, ASIC-resistant networks appear more energy- and carbon-efficient, which complicates any straightforward judgment.

As, ceteris paribus, one can associate hash rate with security, this could be interpreted to mean that ASIC resistance is very inefficient in terms of energy consumption (or other input metrics) “per unit of security”. A counter would be that there are more intangible measures of security than just hash rate, as ASIC-resistant networks could be argued to be more decentralised in terms of retail user accessibility, which is a form of security. However, maintaining this point requires arguing that this form of accessibility of inclusion increases security by orders of magnitude, to compensate for the differences in energy consumption per hash.

Ultimately, the choice between ASIC and ASIC-resistant mining reflects radically different concepts of network security and decentralisation, and associated notions of trade-offs between decentralisation and environmental efficiency. ASIC resistance supports broader participation and potentially enhances network fairness, but at the cost of greater energy and waste intensities That may become indefensible without a radically different concept of security and decentralisation to those held in ASIC coin communities. As the cryptocurrency sector continues to evolve, these environmental and technical considerations will be central to the debate on sustainable and equitable blockchain infrastructure, as well as the environmental impact of the portfolio of ASIC and ASIC-resistant coins.

References

Aponte-Novoa, F.A., Orozco, A.L.S., Villanueva-Polanco, R. and Wightman, P. (2021). The 51% Attack on Blockchains: a Mining Behavior Study. IEEE Access, [online] 9, pp.140549–140564. doi:https://doi.org/10.1109/ACCESS.2021.3119291.

Bertrand, J. (2022). Is ASIC Resistance Necessary for Decentralization in Bitcoin Mining? a Comprehensive Analysis - D-Central. [online] D-Central. Available at: https://d-central.tech/is-asic-resistance-necessary-for-decentralization-in-bitcoin-mining/.

Cambridge Centre for Alternative Finance (2024). Cambridge Digital Mining Industry Report Cambridge Digital Mining Industry Report April 2025 FIRST EDITION Global Operations, Sentiment, and Energy Use Cambridge Digital Mining Industry Report. [online] Available at: https://www.jbs.cam.ac.uk/wp-content/uploads/2025/04/2025-04-cambridge-digital-mining-industry-report.pdf.

Cho, H. (2018). ASIC-Resistance of Multi-Hash Proof-of-Work Mechanisms for Blockchain Consensus Protocols. IEEE Access, 6, pp.66210–66222. doi:https://doi.org/10.1109/access.2018.2878895.

Crypto Analyst (2024). GPU Mining Vs ASIC I Decentralised Mining, Profitability, Efficiency & Flexibility. [online] Crypto Mining Solutions. Available at: https://www.crypto-mining.co.uk/faqs/gpu-mining-explained/.

Dutta, B., Barnita Maity, Banerjee, A. and Mandal, T. (2022). ASIC-Based Mining System in Blockchain for IoT Environment to Increase Scalability and Security. Blockchain, pp.107–121. doi:https://doi.org/10.1201/9781003203957-9.

Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O. and Zvieriev, V. (2023). Evaluating Hashing Algorithms in the Age of ASIC Resistance. [online] Available at: https://ceur-ws.org/Vol-3628/paper15.pdf.

Yap, R. (2018). ASIC Resistance Is Still Worth the Fight for Egalitarian Mining, This Time with Merkle Tree Proofs (MTP). [online] CryptoSlate. Available at: https://cryptoslate.com/asic-resistance-is-still-worth-the-fight-for-egalitarian-mining-this-time-with-merkle-tree-proofs-mtp/.

Authors :

Aayush Ladda, Data Scientist at DLT Science Foundation
Juan Ignacio Ibañez, General Secretary at the MiCA Crypto Alliance
Kamil Tylinski, Head of Data Intelligence at Nodiens & Researcher at University College London
Marco Alberto Javarone, Director of Research & Development at Exponential Science
Paolo Tasca, PhD, Chief Wizard at Nodiens, Associate Professor at University College London & Executive Director at University College London, Centre for Blockchain Technologies

MiCA Crypto Alliance

The MiCA Crypto Alliance, is a strategic initiative aimed at supporting the industry's transition to compliance with MiCA. Bringing together leading blockchain projects such as Ripple, Hedera and Aptos Foundation, the alliance seeks to streamline compliance and enhance regulatory adherence across the crypto market.

This alliance focuses on standardising compliance efforts among its members, offering exclusive resources like sustainability indicators and white paper elaboration tools tailored to meet MiCA requirements. By leveraging the collective expertise of its members, the MiCA Crypto Alliance will help reduce the complexities and costs associated with compliance, while setting a high standard for transparency, market integrity, and consumer protection.For more details on joining the MiCA Crypto Alliance.

Visit: **micacryptoalliance.com**
Contact us: **mica@dltscience.org**

Email address: mica@dltscience.org