Proof of Work Without Heat:

Landauer's Principle and the Economic Origin of Bitcoin's Energy Consumption

Technical note

Théo Couerbe
theo.couerbe@etu.emse.fr

August 2026

Abstract

A popular narrative holds that Bitcoin's energy consumption is physically necessary: that proof-of-work is "anchored in thermodynamics" and that its cost in joules is what makes the ledger trustworthy. This note tests that claim with the correct accounting. Using Landauer's principle, we show that the thermodynamic floor of mining one block is set by the information the protocol actually retains, roughly $\log_2 N \approx 79$ bits for $N \approx 5\times10^{23}$ hash attempts, or about 2×10^{-19} J per block: some 31 orders of magnitude below the network's real dissipation, and reducible further, in principle toward zero, by Bennett's reversible-computing construction. We locate the popular claim's error precisely (a one-bit-per-hash accounting that misapplies both Shannon's and Landauer's definitions), decompose the 10^{31} gap into an economic factor, an algorithmic factor, and a technological factor, and derive the fixed point that actually sets consumption: difficulty adjustment ties network power to miner revenue, not to physics. The interesting consequences are then drawn in the other direction. Proof-of-work certifies computation, not dissipation; its security budget is a flow, linear in expenditure, unlike the exponential, stock-like security of the signatures it protects; and its identification with energy is contingent on today's CMOS operating $\sim 10^4$ times above the Landauer limit. If hardware continues toward that limit, proof-of-work's binding cost migrates from energy to capital, with measurable consequences for its attack model. This yields a falsifiable prediction and reframes the debate: thermodynamics does not justify Bitcoin's energy use, and that negative result is itself the informative one.

1 Introduction

Bitcoin's electricity consumption, of order 10 to 20 GW in recent years [14, 12], is often defended by an appeal to physics. The argument, in its strong form, says that proof-of-work (PoW) performs irreversible computation, that irreversible computation must dissipate heat by Landauer's principle, and that the network's energy bill is therefore a manifestation of physical law: the unavoidable price of trustless consensus. Variants of this claim circulate widely, from informal essays to preprints presenting Bitcoin as a thermodynamically grounded "dissipative structure" [17].

This note takes the claim seriously enough to compute it, and finds that it fails quantitatively by about 31 orders of magnitude and conceptually in its entirety. That is not a reason to abandon the cross-disciplinary question. It is a reason to invert it. The productive question is not "how does thermodynamics justify Bitcoin's energy use?" but "what does it change about proof-of-work that thermodynamics justifies almost none of it?" Three things, we will argue:

1. **Accounting.** The thermodynamic floor of mining is set by the information the protocol retains, not by the number of hashes computed. Done correctly (Section 3), the floor is $\sim 2 \times 10^{-19}$ J per block, and Bennett's result on reversible computation [2] pushes even

this toward zero in principle. The gap between floor and reality decomposes cleanly into an economic factor ($\sim 10^{24}$), an algorithmic factor ($\sim 10^{3}$), and a technological factor ($\sim 10^{5}$), none of which is physical law (Section 4).

2. **Economics.** What actually pins down consumption is a fixed point created by difficulty adjustment: free entry drives mining expenditure toward miner revenue, so power tracks the bitcoin price and the fee market, not any physical constant (Section 5). Efficiency improvements do not reduce consumption; they are absorbed by difficulty.

3. **Security semantics.** If dissipation is not physically required, then PoW is a proof of *computation*, and only contingently a proof of *energy*. The identification of the two rests on CMOS technology operating $\sim 10^{4}$ times above the Landauer limit per switching event. Should that margin close, as the Koomey trend suggests it slowly does [7], the binding cost of mining migrates from operating expenditure (energy) to capital expenditure (hardware), which changes the attack economics of the system (Section 6). This is a falsifiable claim about the future of PoW, and it is reached only by making the physics and the economics talk to each other.

Throughout, we are explicit about which statements are theorems, which are estimates, and which are interpretations. Section 9 positions the note against three existing strands of literature.

2 Thermodynamics of computation in two results

We need exactly two results from the physics of computation, both standard.

Theorem 1 (Landauer [1])**.** *Any physical implementation of a logically irreversible operation, in contact with an environment at temperature T, must dissipate at least $k_{\mathrm{B}}T\ln 2$ of heat per bit of information erased.*

Proof sketch. Resetting a bit of unknown value to 0 halves the number of accessible microstates of the memory, reducing its Gibbs entropy by up to $k_{\mathrm{B}}\ln 2$. The second law requires the environment's entropy to increase by at least as much, and at temperature T an entropy increase ΔS requires heat $Q = T\,\Delta S \geq k_{\mathrm{B}}T\ln 2$. The bound is saturated only in the quasistatic limit; finite-speed erasure dissipates strictly more (Section 7). At $T = 300$ K, $k_{\mathrm{B}}T\ln 2 = 2.87\times 10^{-21}$ J. □

Two details matter below. First, the relevant temperature is that of the heat bath, the ambient environment, not the chip junction temperature: cooling a die does not lower the bound. Second, the bound is per bit *erased*, not per bit processed, stored, or transmitted. Writing onto blank memory, and reversible transformations generally, have no such floor.

Theorem 2 (Bennett [2])**.** *Any computation can be embedded in a logically reversible one that produces the same output, by saving intermediate results and then uncomputing them. The only thermodynamically obligatory erasure is that of whatever memory one insists on resetting; given sufficient blank memory, the dissipation per useful operation can be made arbitrarily small.*

Theorem 2 is the standard resolution of Maxwell's demon [3, 4, 5]: the demon's cost lives in resetting its memory, and a demon with unbounded blank tape defers that cost indefinitely. It is also, as we will see, the theorem that quietly demolishes the "physical necessity" narrative for PoW, because it means logical irreversibility in the algorithm does not force dissipation in the implementation.

3 Three accountings of the mining floor

Fix the network parameters we will use throughout, representative of early 2026: hash rate $H \approx 9 \times 10^{20}$ hashes per second, block interval $\tau = 600$ s, hence expected attempts per block

$$N = H\tau \approx 5.4 \times 10^{23} \approx 2^{78.8}, \tag{1}$$

and measured network power $P_{\text{actual}} \approx 15$ GW [14], i.e. $E_{\text{actual}} \approx 9 \times 10^{12}$ J per block. We now compute the thermodynamic floor three ways, in decreasing order of naivety.

3.1 Accounting A1: one bit per hash

The calculation most often encountered runs as follows. Each hash attempt "answers a binary question" (does this nonce satisfy the target?), hence resolves one bit, hence by Landauer costs at least $k_{\text{B}}T \ln 2$; the floor per block is then

$$E_{\text{A1}} = N k_{\text{B}} T \ln 2 \approx 5.4 \times 10^{23} \times 2.87 \times 10^{-21} \text{ J} \approx 1.5 \times 10^{3} \text{ J}, \tag{2}$$

about 2.6 W of network power. The number looks pleasingly rigorous and is entirely wrong, for two independent reasons.

The one-bit-per-hash fallacy. (i) A binary question carries one bit only if its outcomes are equiprobable. Here the success probability per attempt is $p = 2^{-78.8}$, so the Shannon information of one attempt's outcome is $h(p) \approx p \log_2(1/p) \approx 79 \times 2^{-79}$ bits, about 10^{-22} bits: the outcome "failure" is so predictable that observing it teaches essentially nothing. Summing over N attempts gives $\approx \log_2 N$ bits for the whole search, not N bits. (ii) Landauer's bound charges for erasing *physical memory*, not for eliminating *abstract possibilities*. No miner ever instantiates a 2^{79}-slot register of candidate nonces; there is nothing of that size to erase. The A1 accounting double-counts on both axes at once, and the two errors compound to a factor of $N/\log_2 N \approx 7 \times 10^{21}$.

We single this fallacy out because it is the load-bearing step in most "thermodynamic" defenses of PoW energy use, including, in an earlier form, the author's own first draft of this note.

3.2 Accounting A2: information retained by consensus

The information the search actually produces is the identity of the winning nonce: the entropy of the solution's location, $\log_2 N \approx 79$ bits, is resolved to zero. If the mining hardware is operated conventionally (each attempt's working registers irreversibly overwritten by the next), the honest Landauer floor per block is the cost of retaining those bits while resetting the machinery around them, of order

$$E_{\text{A2}} \approx (\log_2 N)\, k_{\text{B}} T \ln 2 \approx 79 \times 2.87 \times 10^{-21} \text{ J} \approx 2.3 \times 10^{-19} \text{ J per block}, \tag{3}$$

a network power of $\sim 4 \times 10^{-22}$ W. For scale: the entire Bitcoin network, run at this floor, would need 31 orders of magnitude less power than it uses, and 10^{20} blocks could be mined with the kinetic energy of a falling snowflake.

A subtlety worth making explicit: *storing* the block itself (of order 10^6 to 10^7 bits) is not erasure and has no Landauer cost; append-only growth onto blank media is thermodynamically free in the limit. Erasure enters only when memory is reset, for instance when a pruned node deletes an old block, which for a 1 MB block costs at least $8 \times 10^6 \times k_{\text{B}} T \ln 2 \approx 2 \times 10^{-14}$ J. The ledger's thermodynamic bookkeeping is dominated by deletion, not by consensus.

3.3 Accounting A3: the Bennett limit

Even A2 assumes the search is implemented irreversibly. Theorem 2 removes that assumption: a reversible circuit can evaluate each SHA-256d candidate, copy out the one-bit comparison result, and uncompute all intermediates, erasing nothing. With enough blank ancilla memory, or with erasure deferred and amortized, the obligatory dissipation per block approaches the cost of resetting whatever the operator ultimately insists on resetting, which can be made $o(\log_2 N)$ bits. The floor is, in principle,

$$E_{\mathrm{A3}} \longrightarrow 0^{+}, \tag{4}$$

up to finite-speed corrections discussed in Section 7. The conclusion of this section is therefore stark: **thermodynamics imposes no meaningful lower bound on the energy cost of Bitcoin mining.** Whatever explains the 15 GW, it is not physics.

4 Where the 31 orders of magnitude live

The gap between E_{actual} and E_{A2} factors exactly into three terms. Write the actual energy per block as

$$E_{\mathrm{actual}} = N \cdot g \cdot \varepsilon_g, \tag{5}$$

where g is the number of irreversible switching events per hash (for double SHA-256 on a modern ASIC, of order $g \sim 10^5$) and ε_g the energy dissipated per switching event. Current hardware achieves roughly 15 J/TH, i.e. 1.5×10^{-11} J per hash, hence $\varepsilon_g \approx 1.5 \times 10^{-16}$ J. Then

$$\frac{E_{\mathrm{actual}}}{E_{\mathrm{A2}}} = \underbrace{N}_{\substack{\text{economic}\\ \approx 5\times 10^{23}}} \times \underbrace{\frac{g}{\log_2 N}}_{\substack{\text{algorithmic}\\ \approx 1.3\times 10^{3}}} \times \underbrace{\frac{\varepsilon_g}{k_{\mathrm{B}} T \ln 2}}_{\substack{\text{technological}\\ \approx 5\times 10^{4}}} \approx 4 \times 10^{31}. \tag{6}$$

Factor	Magnitude	Set by	Reducible by
N (attempts per block)	$\sim 10^{23.7}$	difficulty $\leftarrow$ economics	nothing physical: see Sec. 5
$g/\log_2 N$ (ops per retained bit)	$\sim 10^{3.1}$	SHA-256d circuit	algorithm choice, reversible logic
$\varepsilon_g/k_{\mathrm{B}}T\ln 2$ (CMOS overhead)	$\sim 10^{4.7}$	semiconductor tech	Koomey trend [7, 8]

Cross-check: 1.5×10^{-11} J/hash $\times$ 9×10^{20} hash/s = 13.5 GW, consistent with measured network power, so the decomposition closes. The striking feature of the table is that the largest factor by far, N, is not an inefficiency at all. It is a protocol variable, retargeted every 2016 blocks precisely so that total work tracks total hash power. Physics cannot compress it, because it was never physical to begin with. Its origin is the subject of the next section.

5 The economic fixed point

Difficulty adjustment makes Bitcoin's energy consumption the solution of an economic equation, not a thermodynamic one. Let R be the block subsidy (3.125 BTC since 2024), F the fees per block, p the bitcoin price, c_E the marginal price of electricity, and s the share of energy in miners' total marginal cost. Free entry and exit of hash power drive expected profit toward zero, so per block

$$\underbrace{(Rp + F)}_{\text{revenue}} \approx \underbrace{\frac{P\, c_E\, \tau}{s}}_{\text{cost}}, \qquad \text{hence} \qquad P \approx \frac{s\,(Rp + F)}{c_E\, \tau}. \tag{7}$$

Every quantity on the right is economic. As an illustration with representative values ($s \approx 0.5$, $c_E \approx 0.05$ USD/kWh $= 1.4 \times 10^{-8}$ USD/J, $F \ll Rp$, and p of order 10^5 USD as observed in 2025 and 2026), equation (7) gives $P \approx 19$ GW, squarely in the measured range. The fixed point reproduces reality; the Landauer bound misses it by 10^{31}.

Equation (7) has a corollary that the efficiency debate persistently gets backwards: **hardware efficiency does not appear in it.** If ASICs halve their J/hash, hash rate roughly doubles, difficulty retargets, N doubles, and P returns to the value set by revenue: a protocol-enforced Jevons effect. Thermodynamic progress changes who mines and with what, not how much energy is consumed. Consumption falls only if revenue falls (price, subsidy halvings, fee market) or if the energy share s of costs falls, which is precisely the migration mechanism of Section 6.

6 Consequences: what proof-of-work actually proves

The negative result of Sections 3 to 5 is where the interesting physics-economics dialogue starts, not where it ends. Three consequences follow.

6.1 Stock security versus flow security

Bitcoin welds together two security mechanisms of entirely different mathematical character. Its signatures are protected by a *stock* of entropy: breaking a key requires $\sim 2^{128}$ operations, an exponential barrier that no budget crosses. Its transaction *ordering*, by contrast, is protected by a *flow*: rewriting recent history requires out-computing the honest network for the duration of the attack, a cost linear in time and expenditure, as Budish has formalized [11]. Thermodynamic language enters only the second mechanism, and, as shown above, only metaphorically. Recognizing the stock/flow split clarifies why "Bitcoin is secured by energy" conflates two unrelated guarantees: the exponential one owes nothing to energy, and the linear one owes nothing to physics.

6.2 Proof of computation, not proof of dissipation

What a block header verifiably certifies is statistical evidence that $\approx 2^D$ hash evaluations were performed. Joules appear nowhere in the verification. The inference "much computation, therefore much energy" passes through the contingent fact that today's switching event costs $\sim 5 \times 10^4\, k_{\mathrm{B}} T \ln 2$. PoW is thus a proof of *computation*; it is a proof of *dissipation* only under a technological assumption external to the protocol. Two category errors dissolve once this is said. First, "Bitcoin is backed by energy": the energy is degraded, not stored; the chain contains no joules, only evidence of foregone alternatives, which is Szabo's unforgeable costliness [10], an economic notion, and gold's as well (the energy of extraction is equally unrecoverable from an ingot). Second, "PoW converts energy into digital order": the entropy reduction achieved by consensus is ~ 79 bits per block (Section 3.2), some 10^{-14} of the entropy exported to the environment; as an entropy transducer, the network is not inefficient, it is simply not one.

6.3 The reversible-computing horizon and the migration to capital

The identification of computation with dissipation has an expiry condition. The Koomey trend [7] halved energy per computation every 1.5 to 2.6 years for six decades; at $\sim 5 \times 10^4\, k_{\mathrm{B}} T \ln 2$ per switching event today, of order fifteen to twenty halvings separate CMOS from the Landauer region, and reversible or adiabatic logic families [8, 2] are not bounded even there. Suppose, for the sake of the limit, $\varepsilon_g \to k_{\mathrm{B}} T \ln 2$ and beyond. Equation (7) still holds: consumption is

set by revenue. What changes is the composition of cost: the energy share s collapses, and the binding expenditure becomes *capital*, silicon, not electricity. Proof-of-work becomes, in cost terms, proof-of-capital.

This is not a semantic nicety; it changes the attack model. Energy-dominated mining makes attacks expensive in *opex*: an attacker must buy a continuous flow (power) that is geographically sticky, politically visible, and unrecoverable. Capital-dominated mining makes attacks expensive in *capex*: the attacker must acquire hardware, which can be rented, resold after the attack (softening the penalty, a scenario Budish analyzes [11]), or stockpiled covertly. The security *quantity* (attack cost $\approx$ honest expenditure) is preserved by the fixed point, but the security *texture* (recoverability, observability, rentability of the attack budget) degrades. Hence a falsifiable prediction, which we offer as this note's main forward-looking claim: **as J/hash falls over the coming decades, the energy share of mining cost will decline, and PoW's practical security will come to depend on the illiquidity of ASIC capital rather than on energy markets; observers should track $\varepsilon_g/k_{\mathrm{B}}T\ln 2$ and the opex/capex ratio of public miners as the two coordinates of that migration.** The popular "energy anchor" narrative silently assumes both coordinates frozen. Physics does not freeze them.

7 Rate limits: what physics does still say

Honesty requires stating the one place thermodynamics genuinely bites: speed. Landauer's bound is attained only quasistatically, and reversible logic dissipates per operation an amount growing with clock rate (in adiabatic charging, roughly proportional to speed [8]). Mining is a race against a 600-second clock, so can miners actually approach the reversible limit? Yes, by trading speed for parallelism: k chips clocked k times slower deliver the same hash rate at lower total dissipation, at the price of k times the silicon. The rate constraint therefore does not rescue the energy narrative; it accelerates the migration to capital of Section 6, since the road to low ε_g is paved with more hardware. For completeness, the ultimate quantum rate limit of Margolus and Levitin [6] allows $\sim 6 \times 10^{33}$ operations per second per joule of system energy; the network's $\sim 10^{26}$ logical operations per second would saturate the bound with well under a microjoule. No fundamental rate limit is within thirty orders of magnitude of relevance.

8 What remains of Maxwell's demon

The demon analogy, common in this literature, survives only as an illustration, and it is worth stating the correct version once. The demon's paradox is resolved by charging it for memory reset [4, 5]; consensus, viewed as a demon, selects one continuation of the chain among candidates and orders transactions within a block. The associated information is tiny: fork selection is usually 0 to 1 bit, and choosing an ordering of $k \approx 3 \times 10^3$ transactions resolves at most $\log_2 k! \approx 3 \times 10^4$ bits, a Landauer cost of $\sim 10^{-16}$ J. Consensus is informationally almost free. What is expensive in a permissionless system is not selecting the history but making *identities* costly, sybil resistance, and thermodynamics is indifferent to which scarce resource plays that role: energy today, capital tomorrow, stake elsewhere. The demon points at the right concept (information has a physical price) and the wrong magnitude (the price here is twenty orders of magnitude below a dewdrop's surface energy).

9 Related work

Three strands frame this note. (i) A metaphorical literature presents Bitcoin as thermodynamically grounded, e.g. as a dissipative structure converting energy into monetary order [17]; our

Sections 3 and 5 quantify why such framings cannot be more than analogy. (ii) A recent quantitative strand studies the entropy of block arrival as a timing mechanism, modeling discovery as Bernoulli/Poisson sampling and entropy collapse at each block [15, 16]; that work concerns the information dynamics of the clock, is compatible with ours, and does not address energy floors. (iii) The energy-economics literature measures and models consumption [14, 12, 13, 11]; we import its fixed-point logic and supply the missing thermodynamic side of the ledger, namely that physics contributes a floor of 10^{-19} J where economics contributes 10^{13} J. The physics-of-computation results used are canonical [1, 2, 3, 4, 5, 6, 7, 8]. To our knowledge, the explicit three-factor decomposition of Section 4 and the opex-to-capex migration argument of Section 6 have not been assembled elsewhere, though each ingredient is standard in its home discipline; that assembly, rather than any single equation, is the contribution claimed here.

10 Conclusion

Confronting Bitcoin with thermodynamics, done carefully, returns a verdict opposite to the popular one. Landauer's principle prices the information consensus retains at $\sim 10^{-19}$ J per block; Bennett's construction lowers even that; the observed 15 GW is fixed by a revenue equation in which no physical constant appears. Proof-of-work is a proof of computation whose energy character is a property of 2026 semiconductors, not of nature, and the system's security texture will migrate from energy markets to capital markets to the extent that hardware keeps approaching the Landauer region. None of this diminishes the interest of the encounter between the two fields; it relocates it. The physics does not explain the megawatts. It explains, instead, exactly which parts of Bitcoin's design are contingent, which are economic, and which, like the 79 bits a block is really worth, are almost nothing at all.

References

[1] R. Landauer, "Irreversibility and Heat Generation in the Computing Process," *IBM Journal of Research and Development*, vol. 5, no. 3, pp. 183-191, 1961.

[2] C. H. Bennett, "The Thermodynamics of Computation: a Review," *International Journal of Theoretical Physics*, vol. 21, no. 12, pp. 905-940, 1982.

[3] L. Szilard, "Über die Entropieverminderung in einem thermodynamischen System bei Eingriffen intelligenter Wesen," *Zeitschrift für Physik*, vol. 53, pp. 840-856, 1929.

[4] C. H. Bennett, "Notes on Landauer's principle, reversible computation, and Maxwell's demon," *Studies in History and Philosophy of Modern Physics*, vol. 34, no. 3, pp. 501-510, 2003.

[5] T. Sagawa and M. Ueda, "Minimal Energy Cost for Thermodynamic Information Processing: Measurement and Information Erasure," *Physical Review Letters*, vol. 102, 250602, 2009.

[6] N. Margolus and L. B. Levitin, "The maximum speed of dynamical evolution," *Physica D*, vol. 120, pp. 188-195, 1998.

[7] J. Koomey, S. Berard, M. Sanchez, and H. Wong, "Implications of Historical Trends in the Electrical Efficiency of Computing," *IEEE Annals of the History of Computing*, vol. 33, no. 3, pp. 46-54, 2011.

[8] M. P. Frank, "The Physical Limits of Computing," *Computing in Science & Engineering*, vol. 4, no. 3, pp. 16-26, 2002.

[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[10] N. Szabo, "Shelling Out: The Origins of Money," essay, 2002.

[11] E. Budish, "The Economic Limits of Bitcoin and the Blockchain," NBER Working Paper 24717, 2018.

[12] A. de Vries, "Bitcoin's Growing Energy Problem," *Joule*, vol. 2, no. 5, pp. 801-805, 2018.

[13] R. Auer, "Beyond the doomsday economics of 'proof-of-work' in cryptocurrencies," BIS Working Papers No. 765, Bank for International Settlements, 2019.

[14] Cambridge Centre for Alternative Finance, "Cambridge Bitcoin Electricity Consumption Index," `https://ccaf.io/cbnsi/cbeci`, accessed 2026.

[15] "Bitcoin: A Non-Continuous Time System," arXiv:2501.11091, 2025.

[16] "Entropy-Based Evidence for Bitcoin's Discrete Time Mechanism," TechRxiv preprint, 2026.

[17] "Bitcoin Well Theory: A 3D Thermodynamic Perspective," Zenodo preprint 14686888, 2025.